Federal Mobility Group

November 2020

Acknowledgements

Contributing Departments, Agencies, and Organizations

Department of Defense – Air Force

Department of Defense – Defense Information Systems Agency

Department of Defense – National Information Warfare Center – Pacific / Atlantic

Department of Defense – Office of Secretary of Defense

Department of Defense – U.S. Navy

Department of Energy

Department of Energy – Idaho National Lab

Department of Homeland Security – Cybersecurity and Infrastructure Security Agency

Department of Homeland Security – Science & Technology

Department of Treasury

Environmental Protection Agency

General Services Administration

National Aeronautics & Space Administration

National Institute of Standards and Technology

National Science Foundation

National Security Agency

National Telecommunications and Information Administration

Office of Management & Budget

Office of Science and Technology Policy – Networking and Information Technology Research and Development

Office of Science and Technology Policy (The White House)

State Department

The MITRE Corporation

U.S. Agency for International Development

Executive Summary

The International Mobile Telecommunications Vision 2020[1] defines three usage scenarios for fifth generation (5G) telecommunications that distinguish 5G from fourth generation (4G). The scenarios are enhanced mobile broadband (eMBB), ultra-reliable, low-latency communications (URLLC), and massive machine-type communications (mMTC), also referred to as massive Internet of Things (mIoT).

Federal agencies are exploring how to take advantage of 5G to improve mission delivery and business operations and deliver new applications and services that are not achievable with current 4G technology. The Federal Mobility Group's (FMG) 5G and Mobile Network Infrastructure Working Group (WG) undertook an evaluation of 5G testing approaches to understand available 5G testing capabilities to avoid duplication, promote the use of shared testing resources, and define a framework for federal 5G testing.

Delivering 5G's capabilities requires significant changes to mobile communication systems. These changes can introduce security vulnerabilities and expand the attack surface. *The National Strategy to Secure 5G* and the implementation plan for the *Strategy* define four lines of effort to secure 5G infrastructure and systems. The WG's 5G testing efforts align to the *National Strategy's* "facilitate domestic 5G rollout" line of effort and its aim of promoting the research, development, testing, and evaluation of new technologies and architectures that advance 5G technology via access to shared test resources.

To survey and collect information about available 4G/5G testing capabilities, the WG worked with cellular equipment manufacturers, mobile network operators, federal labs, and academia to visit their labs. The WG members received overviews, demonstrations, and lab walkthroughs at each site and reached the following conclusions regarding lab capabilities and suitability for use by the federal government:

- Equipment Manufacturer Labs
  - Good option for federal government testing needs.
  - Equipment conforms to Third Generation Partnership (3GPP) standards and continues to evolve with standards.
- Mobile Network Operator Labs
  - Internal integration labs are used for testing prior to deployment of services and are generally not available for government testing.
  - External labs for application development and innovation are open to the public, but typically for small-scale, light use.
  - Agencies could work with carriers for temporary use of licensed 5G spectrum.
- Federal Labs
  - Option for open-field outdoor testing and specific/sensitive test requirements and scenarios.
  - Straightforward approach for federal agency use.
  - Federal labs currently use 4G with plans to upgrade to 5G.
- University Labs and Testbeds
  - Option for conceptualization, mid-to-long-term research and development (R&D), and campus testing (outdoor testing and city-scale testbeds).

This document recommends a framework to conduct 5G testing. The framework builds on the insights gained from the lab visits and proposes a modular approach to support the diverse needs of different federal use cases and explore the new and enhanced capabilities of 5G. To develop the elements of the framework, the WG scanned the federal landscape and identified 60 5G-releated initiatives, which were grouped into subject areas (e.g., infrastructure, policy and standards, R&D, security, spectrum, supply chain). Next, WG members were surveyed to identify additional envisioned uses for 5G and provide details for each use case such as 5G usage scenario, type and number of connected devices, operating environment, type of traffic and data sensitivity, and anticipated operating spectrum. WG members from the Departments of Defense and Homeland Security submitted 11 use cases; some are very broad while others are very focused.

1 Recommendation ITU-R M.2083-0. "IMT Vision – Framework and overall objectives of the future deployment of IMT for 2020 and beyond." International Telecommunications Union. September 2015. Online: https://www.itu.int/rec/R-REC-M.2083- 0-201509-I/en (Link accessed May 15, 2020).

The intent of collecting federal initiatives and use cases was to identify commonalities across agencies and define a framework that supports testing of different use cases and builds on the capabilities available from 5G labs and testbeds visited by the WG. The characteristics of the federal initiatives and the WG's use cases indicate that federal agencies want to take advantage of many of the features and capabilities that 5G has to offer. Because 5G architecture makes extensive use of softwarization and virtualization and will rely on existing 4G technology for at least the next several years, all agencies also have an interest in understanding 5G security features and security risks.

The framework identifies the capabilities and elements needed to conduct 5G testing and provides a process an agency could use to identify which testing capabilities are necessary for its use case. The framework includes:

- End-to-end 5G testing architecture and mapping to 3GPP 5G Standards.
- A modular approach listing all possible testing elements needed for different use cases.
- Two examples of how to use the framework to understand the test elements and determine which ones are needed for a particular use case.
- Performance and security metrics that can be collected on a 5G testbed.

The 5G testing architecture is divided into four main phases, notionally based on the timeline for 3GPP 5G standards releases and 5G equipment/device vendor offerings. The first phase, for example, implements the 5G non-standalone architecture, which relies on existing 4G core network infrastructure, while the second phase upgrades the network core to 5G in a standalone mode. The modular elements of the framework are organized by architecture, spectrum, application traffic, network, and 5G innovations. Each subsection includes a description and considerations for the test element as well as associated test and measurement equipment (e.g., protocol analyzer). Not all elements are required for all testing; for example, an emulated Radio Access Network (RAN) can be used if a real RAN is not available. The framework concludes with a summary of the security considerations for the framework and security metrics an agency could collect via the framework.

After using the framework, an agency could establish a testing capability suited to its needs by building/leasing a testbed from a carrier-grade equipment manufacturer, using existing external labs/testbeds (e.g., federal lab, university lab, coordination with Department of Defense) to conduct testing, or using a combination.

The framework supports activities related to collaboration and promotion of shared lab capabilities in the *National Strategy to Secure 5G Implementation Plan*. While the framework is intended to support coordination of 5G test activities across the federal government, the process for developing the framework and defining its modular elements can be applied more broadly to both public- and private- sector enterprises. FMG is working with the Networking and Information Technology R&D subcommittee to determine how to leverage the framework and the testbed assessment for *Implementation Plan* activities related to shared testing resources

Table of Contents

Tables

Figures

This page intentionally left blank

1. Introduction

This document defines a framework to conduct testing and evaluation of fifth generation (5G) mobile technology. Its purpose is to inform federal 5G project managers and testing managers of the breadth of 5G-releated activities within the federal government, describe additional federal use cases, define the key elements and capabilities needed to conduct testing, and promote the use of shared testing resources.

The modular framework builds on the insights gained from visits to fourth generation (4G)/5G labs and proposes a modular approach to support the diverse needs of the different federal use cases and federal initiatives and explore the new and enhanced capabilities of 5G. The framework provides a process an agency could use to establish a testing capability suited to its needs by identifying the capabilities needed for its use case and building/leasing a testbed from a carrier-grade equipment manufacturer, using existing external labs/testbeds, or a combination of the two

1.1 Document Structure

The document is organized as follows:

- A survey of the current federal landscape of 5G-related initiatives and investments to understand the breadth and focus areas of these efforts (Section 2).
- 5G use cases and testing needs submitted by members of the 5G and Mobile Network Infrastructure (MNI) Working Group (WG) representing the Departments of Defense and Homeland Security (Section 3).
- Summary of capabilities discovered through the 4G/5G testbed assessment and the strengths of each type of lab visited by the WG (Section 4).
- A modular framework that defines key capabilities to support testing of a broad variety of federal test cases and a process showing how to use the framework. (Section 5).
- Summary and conclusion. (Section 5).
- A brief overview of 5G (Appendix A).
- A detailed list of the federal 5G initiatives that are summarized in Section 2, with agency, focus area, and links for additional information (Appendix B).

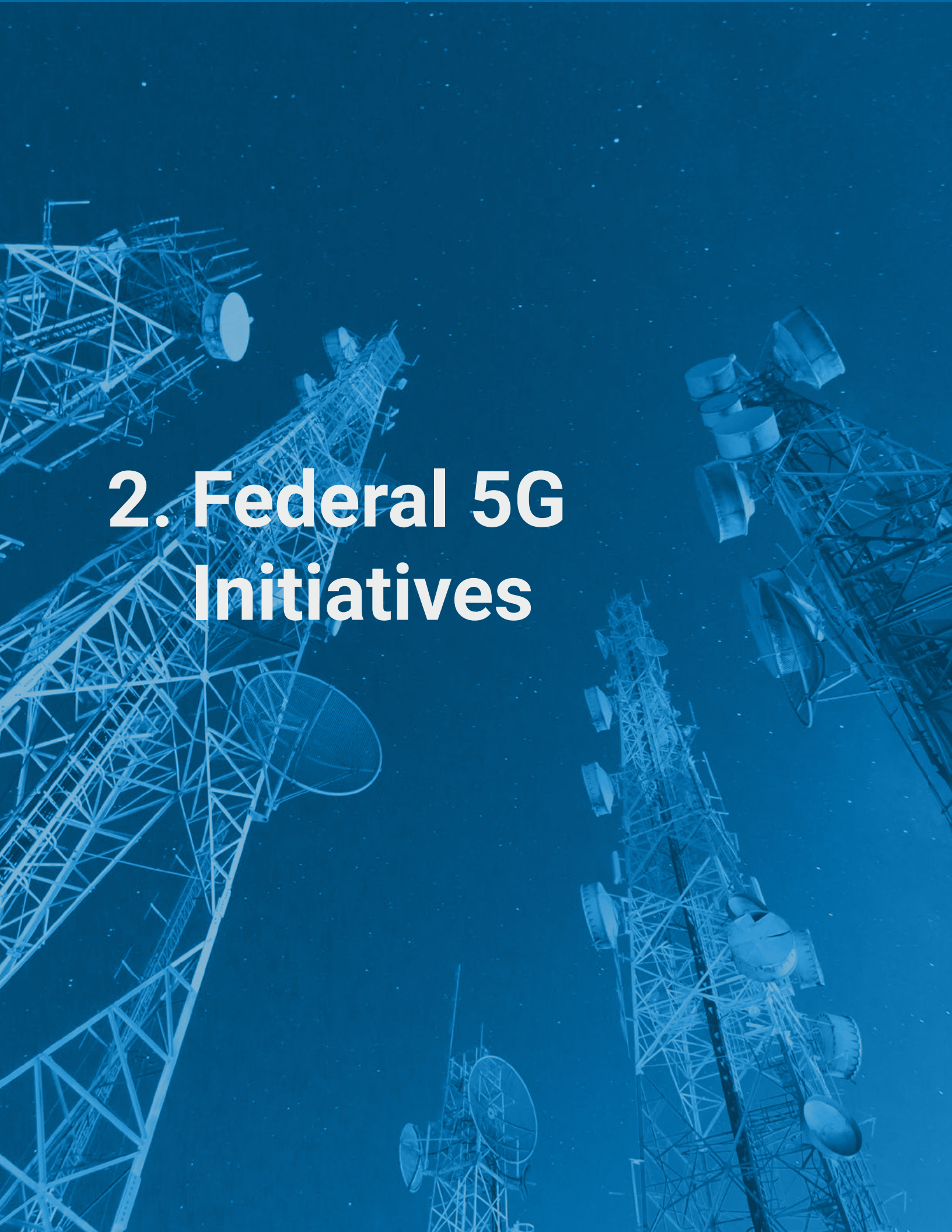
The WG's efforts to catalog capabilities of a set of labs and testbeds and to define a framework for 5G testing align to the "facilitate domestic 5G rollout" line of effort in the National Strategy to Secure 5G and the activities outlined in the National Strategy to Secure 5G Implementation Plan that promote collaboration via access to shared testbeds.

1.2 Background

The Federal Mobility Group (FMG), chartered under the Federal Chief Information Officer (CIO) Council, is organized into four working groups. Its 5G and MNI WG was formed to:

"Coordinate Federal Government position and action related to the maturation and implementation of secure 5G networks and technologies with the primary goals of maximizing the utility, minimizing the public cost, and having a profoundly positive influence on next-generation communications infrastructure development and deployment."

As part of its work program, the Federal CIO Council recommended that the 5G and MNI WG evaluate 5G testing approaches. The WG split this task into two efforts: an assessment of 4G/5G labs and testbeds that was completed in April with findings and insights summarized in Section 4, and development of the testing framework recommended in this document.



2. Federal 5G Initiatives

A review and analysis of current federal initiatives, programs, projects, and working groups shows 60 federal initiatives directly or indirectly associated with 5G, with more than half led by the Departments of Defense (DoD), Commerce (DOC), and the National Science Foundation (NSF). The initiatives have been grouped into seven subject areas to aid in discussion and future research. Reflecting the current state of 5G technologies, one-third of the initiatives are focused on 5G R&D. Figure 1 provides an overview of the initiatives within each department/agency and subject area:

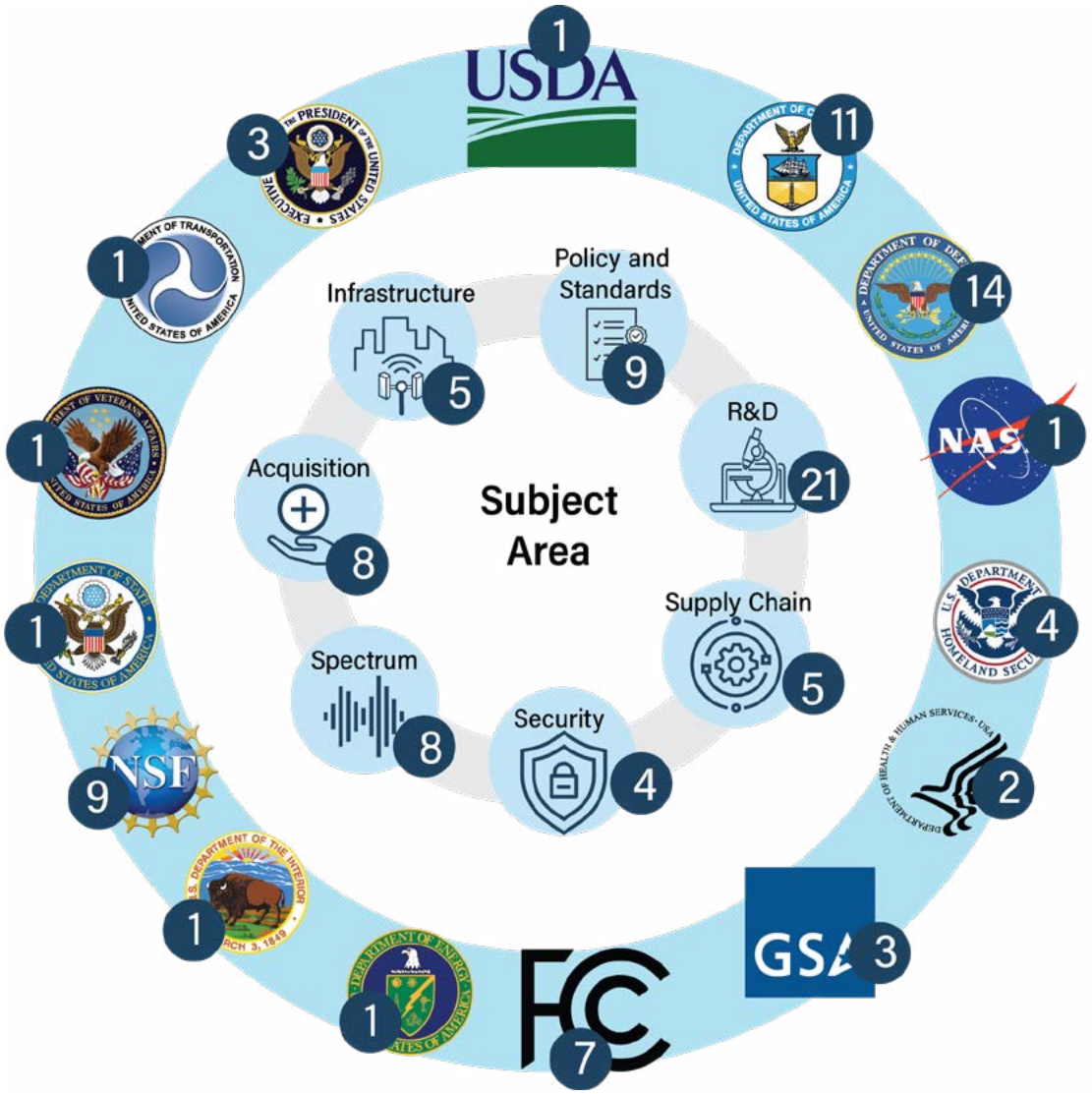


Figure 1. 5G-Related Initiatives by Agency and Subject Area

Sections 2.1 through 2.7 summarize the 5G initiatives federal agencies are engaged in by subject area. Refer to A.2 for a detailed listing of each initiative. Sorted by subject area, each listing includes sponsoring agency, sub-organization, type of initiative (e.g., program, project, working group), subject area, and external links for additional information.

2.1 Acquisition

Four agencies (DoD, GSA, Health and Human Services [HHS] and the National Aeronautics and Space Administration [NASA]) have acquisition initiatives that include mobility products and services such as wireless carrier services, mobile devices, mobile hardware/infrastructure, and IoT. z

The Army operates Computer Hardware Enterprise Software and Solutions (CHESS) and the Navy operates the Wireless Spiral III Program. The General Services Administration (GSA) operates the Technology Modernization Fund's (TMF) Program Management Office (PMO). The TMF PMO works with agencies to build technology modernization business cases and aids in all phases of the acquisition lifecycle. GSA is also overseeing the Federal Strategic Sourcing Initiative for Wireless. A broader portfolio of mobility solutions is available on IT Schedule 70 through an enhanced Special Item Number. By executive order, GSA is coordinating all wireless telecommunications installations on federal property and has consolidated a number of forms, leases, and contracts to help speed the deployment of wireless infrastructure. These processes should be used for buildings or land owned or operated by GSA or agencies directly.

HHS's National Institutes of Health (NIH) has several Government-Wide Acquisition Contracts (GWACs) for procurement of IT, including wireless carrier services, devices, infrastructure, and IoT. NASA manages the Solutions for Enterprise Wide Procurement (SEWP) GWAC contract vehicle has commercial IT products and services that include carrier services, devices, infrastructure, IoT.

2.2 Infrastructure

The infrastructure area touches on any hardware within the system—from transmitters and receivers to core systems and user equipment, including drones/Internet of Things (IoT). The Departments of Agriculture, DOC, DoD, Energy, Homeland Security (DHS), and Transportation each are working on 5G infrastructure. These efforts include both pilots and larger initiatives, ranging from deployment of infrastructure to buildout of existing Long Term Evolution (LTE) networks and upgrade to 5G.

Two agencies are studying the use of 5G with drones. The Department of Agriculture wants to create next-generation geographic information systems to assist with precision agriculture. The Department of Energy is seeking to make research operational. Its researchers have developed a novel 5G wireless network using newly available millimeter wave (mmWave) frequency to operate drones with machine-to-machine communication to provide improved radio frequency (RF) coverage and resiliency against cyberattacks.

The DoD is modernizing bases to use smart technology. This effort includes new infrastructure for mobility, cloud access, unified communications, voice, broadband, Wi-Fi expansion, and an array of connected devices.

The Department of Transportation is working on automated driving systems, intelligent transportation systems, and cellular vehicle-to-everything (V2X) communication. DOC's Institute for Telecommunication Sciences within the National Telecommunications and Information Administration (NTIA) is planning further buildout of their LTE and 5G laboratory and will focus on open RAN and open source implementation of LTE and 5G network elements. DOC's First Responder Network Authority (FirstNet) is working on building out Band 14 of the 700 megahertz (MHz) spectrum nationwide while also investigating how to transition that band to use 5G.

2.3 Policy and Standards

Efforts in this area address the shaping or implementation of various policies and standards. The White House has established the 5G Policy Coordination Committee (PCC) to coordinate federal agency engagement with the 3GPP. One of its sub-PCCs is defining the strategy for 5G and information and communication technology standards adoption.

The FCC and the Department of the Interior (DOI) initiatives are working on 5G deployment and security. DOI has the lead in implementing the executive order for rural broadband deployment. The FCC's plan to Facilitate America's Superiority in 5G Technology is working to push more spectrum into the marketplace, update infrastructure policy, and modernize outdated regulations. Subsequent to the FCC's ban on use of Universal

Service Funds (USF) to purchase hardware, software, or services from companies that pose a national security threat, the FCC is collecting information to determine the extent to which hardware and software from such companies has been used in USF-funded communications networks to inform future actions.

The FCC's Technological Advisory Council (TAC) provides technical advice to the FCC. The TAC's diverse array of leading experts helps the FCC identify important areas of innovation and develop informed technology policies. TAC working groups are established each year. In 2020, all four of its working groups are involved with 5G: 5G RAN technology; future of unlicensed operations; AI; and 5G, IoT, and Open RAN (O-RAN).

The National Institute of Standards and Technology (NIST) is working on securing mobile devices and data and providing guidance on security of cellular technologies. DoD has established technical teams to tackle various 5G standards topics to help create uniformity across the department. DoD is also working with the Five Eyes Alliance to coordinate standards implementation and uniformity.

NTIA's Institute for Telecommunication Sciences (ITS) has developed the leading implementation of the Institute of Electrical and Electronics Engineers (IEEE) 802.15.22.3 standard for Spectrum Characterization and Occupancy Sensing. ITS maintains a Boulder Wireless Test City where spectrum monitoring technologies are developed and tested to detect, geolocate, and mitigate radio interference.

2.4 Research and Development

The subcommittee on Networking and Information Technology Research and Development (NITRD), under the White House National Science and Technology Council, has 11 working groups. The NITRD Wireless Spectrum Research and Development (WSRD) Interagency Working Group (IWG) coordinates Federal spectrum-related R&D and has established an Advanced Wireless Test Platform (AWTP) Team. The WSRD IWG is currently tracking 306 projects that have been completed or are scheduled to be completed from 2018 through 2021. DoD, DHS, NSF, and the Department of Veterans Affairs (VA) are engaged in R&D efforts.

The DoD wants to rapidly take full advantage of 5G capabilities, address security challenges that 5G presents, and begin investments that will advance 5G to the next generation of mobile information technology (IT). Under Tranche 1 of its "5G to Next G" initiative, DoD awarded $600 million for 5G experimentation and testing at five installations. The projects are augmented reality/virtual reality (AR/VR) for training, smart warehouse and asset management (see Figure 2 on the next page), 5G Dynamic Spectrum Sharing (DSS), and a private 5G cellular network at Nellis Air Force Base in Nevada, which will have movable cell towers that can be set up and removed in less than an hour.

An additional seven military installations have been selected in DoD's "second tranche" of testbeds to explore ship-wide/pier connectivity; aircraft mission readiness; bidirectional spectrum sharing; and security. The DoD's Information Warfare Research Project (IWRP) will seek commercial software prototypes for testing on the private network at Nellis Air Force Base. The prototypes will focus on applications and services for survivable command and control and for wireless network enhancements.

The Defense Advanced Research Projects Agency (DARPA) created the Open, Programmable, Secure 5G (OPS-5G) program to tackle many of the security challenges facing future wireless networks. OPS-5G will explore the development of a portable, standards-compliant network stack for 5G mobile

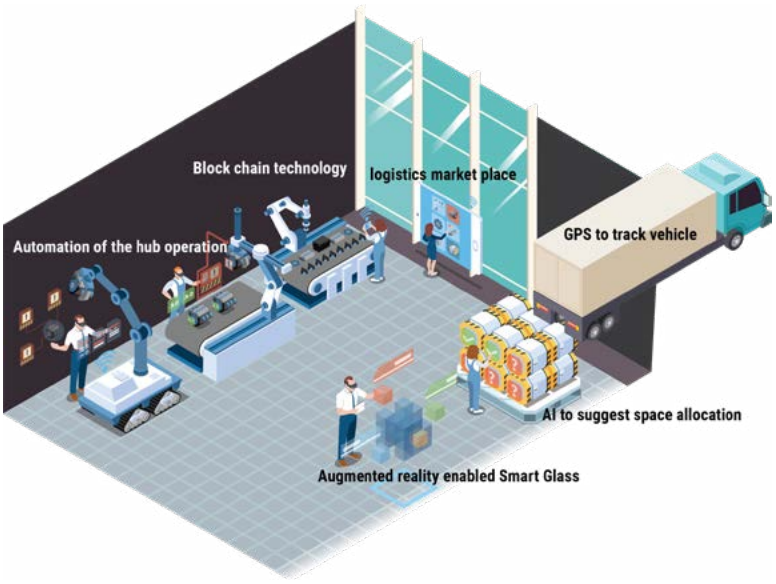


Figure 2. Smart Logistics Management Concept

networks that is open source and secure by design. DoD also continues to support the 5G Secure Profile Working Group, which is developing common parameters for secure standards implementation

Collaboration Challenge (SC2). Competitors developed innovative solutions for autonomous spectrum management in the form of collaborative intelligent radio networks. The goal was to develop new ways to share RF spectrum, thus avoiding interference and exploiting opportunities to achieve the most efficient use of spectrum resources. DoD has invested $2.7 million in a joint DoD/NSF spectrum sharing project. Colosseum, the emulator developed in SC2, was transferred to NSF and is being integrated into the PAWR program ecosystem. Colosseum will be used in the joint spectrum sharing project to explore the use of AI to allocate spectrum resources, with an initial focus on maximizing the use of CBRS spectrum on a live 5G New Radio (NR) network.

Figure 3. COSMOS Base Station Deployment Plan

DARPA is also running the Millimeter-Wave Digital Arrays (MIDAS) program. This program aims to create the technology to enable next-generation DoD millimeter wave systems. MIDAS is focused on two key technical areas: the development of core complementary metal-oxide-semiconductor chips and integrating those chips to create an array composed of MIDAS building blocks that is capable of demonstrating digital multi-beam functionality.

The Defense Information Systems Agency (DISA) runs the Spectrum Access Research & Development Program for new and innovative methods to share spectrum and reduce DoD's overall spectrum footprint.

The DHS secure and resilient mobile network infrastructure R&D program has projects aimed at addressing weaknesses in legacy and 4G networks, techniques to provide a flexible 5G security architecture and security policy for government environments, and improving enterprise visibility and management of mobile network traffic. DHS is also conducting research that will help mitigate threats to unmanned aerial systems.

The National Science Foundation (NSF) has a number of R&D programs including: the Platforms for Advanced Wireless Research (PAWR), the Partnership on Machine Learning for Wireless Networking Systems (MLWiNS), and the National Center for Wireless Spectrum Research (Spectrum Innovation Initiative [SII]-Center). PAWR will support up to four facilities for experimentation with advanced wireless techniques at city-scale and in the wild. PAWR is a public-private partnership funded by NSF and a consortium of 32 wireless companies. The program has funded three platforms as of August 2020: the Cloud Enhanced Open Software Defined Mobile Wireless Testbed for City-Scale Deployment (COSMOS) in New York City (Figure 3 on the following page shows the COSMOS base station deployment plan); the Platform for Open Wireless Data-driven Experimental Research (POWDER) in Salt Lake City; and the Aerial Experimentation and Research Platform for Advanced Wireless (AERPAW) in Research Triangle Park, North Carolina. PAWR will fund one more platform to support research on the efficient delivery of rural broadband by Spring 2021.

MLWiNS is a partnership with Intel to advance machine learning (ML) for wireless networking, spectrum management, and distributed ML over wireless edge networks. The SII-Center, a program under the Spectrum Innovation Initiative, will create a national facility addressing questions relevant to spectrum research, innovation, and workforce development as described in national-level strategy documents

NSF has three additional R&D programs: Communications and Information Foundations Core

Program, Computer and Network Systems Core Program, and Communications, Circuits and Sensing Systems Program. NSF also funded a Millimeter Wave Research Coordination Network (RCN) in 2017 that created a coordination network across academia, national labs and industry in the area of mmWave wireless

communications. Its current research focus is achieving multi-Gigabit data rates and low latency as part of the emerging vision for 5G and beyond wireless systems.

NSF also runs wireless security R&D programs: the Secure and Trustworthy Cyberspace (SaTC) program and the Spectrum Efficiency, Energy Efficiency and Security (SpecEES) and Spectrum and Wireless Innovation enabled by Future Technologies (SWIFT) program. SpecEES and SWIFT seek methods to ensure that spectrum sharing users can communicate securely and that accidental or intentional abuse of spectrum can be detected and mitigated. Security and privacy investments include projects for jamming attack and defense, anonymization and privacy methods, secure localization and location privacy, covert channel detection, distributed denial-of-service (DDoS) defense, and key management and public key infrastructure for networks.

VA and DoD are researching new uses for 5G technology. At Fort Carson, Colorado, DoD is testing the viability of autonomous vehicles and sensor-based technologies in an effort to reduce military transportation costs, deliver faster services on site, and improve overall public safety. VA is studying how to expand telemedicine, connected health, smart medical devices, and artificial intelligence (AI)-assisted electronic health records.

2.5 Security

Each element of 5G systems (RAN, core, hardware, software, spectrum use, user equipment, and applications) represents unique security challenges. Thus, security topics necessarily overlap with other initiative areas. FCC, DOC, and DoD have established working groups to specifically address security.

With NIST's project on 5G cybersecurity at the National Cybersecurity Center of Excellence (NCCoE), DOC is developing approaches and proposed solutions in collaboration with a community of interest, equipment vendors, and telecommunication providers. These solutions are meant to address several security considerations as industry is preparing to migrate to 5G technology.

In its role as the nation's risk advisor, DHS's Cybersecurity and Infrastructure Security Agency (CISA) is leading risk mitigation efforts by working with government and industry partners to ensure the security and resiliency of 5G technology and infrastructure. CISA's 5G Strategy, Ensuring the Security and Resilience of 5G Infrastructure in Our Nation, establishes five strategic initiatives to address critical risks to secure 5G deployment.

2.6 Spectrum

Spectrum usage and research are key 5G focus areas with activities led by FCC, DOC and DoD. NTIA within DOC manages U.S. spectrum for government applications (the FCC does the same for non- government use of spectrum).

One of the FCC's missions is to encourage the highest and best use of spectrum domestically. It also oversees spectrum auctions to sell transmission rights in the U.S. In March 2020, the FCC completed an auction of mmWave spectrum, the largest amount of spectrum ever offered in U.S. history, a step the FCC took to maintain U.S. leadership in 5G. The FCC also recently concluded an auction of low-power mid-band spectrum (Citizens Broadband Radio Service [CBRS]) for 5G services and will be holding an auction of C-Band spectrum at the end of 2020 and S-Band spectrum at the end of 2021.

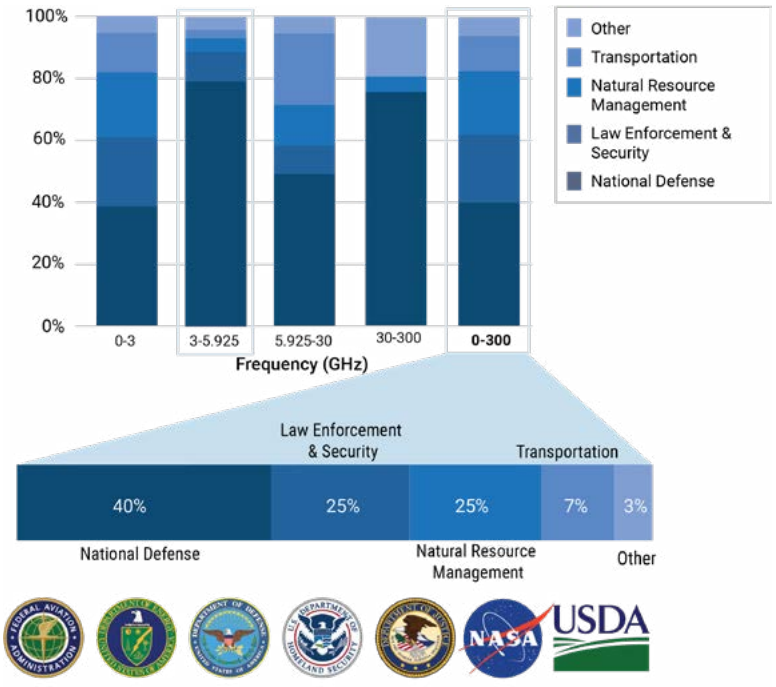


Figure 4. Federal Government Spectrum Usage

NTIA has a number of committees and working groups focused on current and future use of spectrum (e.g., the Interdepartment Radio Advisory Committee, Policy and Planning Steering Committee, Spectrum Strategy Task Force, and Commerce Spectrum Management Advisory Committee). Two of its initiatives are focused on implementing the presidential memo for a national spectrum strategy and the Broadband USA program to expand connectivity across nonprofits and local and state governments. Figure 4 shows how the federal government uses spectrum for its missions.[2]

NTIA/ITS has developed an official propagation code library as a means to standardize propagation models and implementations. ITS also has expertise in government radio systems and works to evaluate interference protection criteria via simulation, laboratory tests, and field tests. NIST is sponsoring the 5G Millimeter-Wave Channel Model Alliance. This research consortium seeks to produce more accurate and predictive channel models, calibrations, and measurements—a key enabler required to support the commercialization of next-generation wireless networks (5G and beyond).

Under DoD's "5G to Next G" initiative, the Air Force Research Laboratory is providing technical and programmatic leadership to establish a 5G network testbed, as well as spectrum sharing and coexistence technologies to enhance dynamic spectrum sharing and spectrum co-existence capabilities. This program aims to develop hardware, software, and systems that can support spectrum sharing and coexistence between a 5G network and radar systems.

2.7 Supply Chain

Federal agencies are pursuing multiple strategies to facilitate the rollout of safer and trusted 5G networks across the country. A primary concern is using equipment from manufacturers who are headquartered in nations that do not align with Western values. Those manufacturers are more likely to have close ties to their governments and intelligence services and hence their hardware, devices, software, or firmware may not be trustworthy enough for use in U.S. critical infrastructure. The FCC, DoD, DHS, and the Department of State have initiatives focused on these concerns.

Figure 5. Information and Communication Technology Supply Chain Phases

The Alliance for Telecommunication Industry Solution's (ATIS) formed the 5G Supply Chain Working Group at the request of DoD. The working group hopes to extend the development of 5G best practices and guidelines to create supply chain standards that can be operationalized in the public and private sectors.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) has established the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force. The ICT supply chain ecosystem encompasses the entire life cycle of ICT hardware, software, and managed services and vulnerabilities can be introduced at any phase of the ICT supply chain (shown in Figure 5). Participants in the ICT SCRM Task Force include 20 federal partners and 40 of the largest companies in the ICT sectors. The public-private supply chain risk management partnership is entrusted with the critical mission of identifying and developing consensus strategies to enhance ICT supply chain security.

2 Adapted from "Basic Elements of Spectrum Management. How the Spectrum is Used." https://www.ntia.doc.gov/legacy/osmhome/roosa2.html (Link accessed August 14, 2020).

The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) provides recommendations on security, reliability, and interoperability of communications systems. Half of the Council's 2020 working groups are related to 5G, including the Managing Security Risk in the Transition to 5G; Managing Security Risk in Emerging 5G Implementations; and Improving Broadcast Resiliency. These working groups aid the Council in the development of best practices and recommendations.

"5G Clean Path," the first effort under the Department of State's "5G Clean Networks" initiative, requires a "Clean Path" for all 5G network traffic entering and exiting U.S. diplomatic facilities. 5G Clean Path envisions an end-to-end communication path that does not use transmission, control, computing, or storage equipment from untrusted IT vendors.

3. Federal Use Cases and Testing Scenarios for 5G Technology

The variety of federal initiatives described in the previous section is indicative of the significant interest that federal agencies have in exploring how to take advantage of, secure, and transition to 5G technologies. The following section describes 5G use cases submitted by members of the 5G and MNI WG. While the initiatives described in Section 2 are currently underway, the use cases described below envision use of 5G features and capabilities to improve mission delivery and business operations as well as to deliver new applications and services that are not achievable with current technology. To round out the use case examples, Section 3.2 reiterates the DoD's "5G to Next G" projects and other federal use cases discussed in Section 2. Section 3.3 summarizes common characteristics of the use cases and initiatives as the basis for the test capabilities needed for the framework.

3.1 Use Cases Defined by 5G and MNI Working Group Members

The 5G and MNI WG developed a questionnaire for its members to document their agency's known or potential use cases or desired applications for 5G. Questions included which usage scenario the use case aligns to, the type of user equipment and number of connected devices, operating environment and size, type of traffic and data sensitivity, mobility, security requirements, performance parameters, and anticipated operating spectrum. WG members from DoD and DHS submitted 11 use cases—some very broad and others very focused. While not intended to be an exhaustive list of potential federal uses for 5G, the submitted use cases summarized below provide insight and additional detail on some ways to harness 5G capabilities:

Autonomous Vehicle Proving Grounds. Create an environment to test multi-modal transit with objectives of lowering cost and environmental impact. User equipment includes autonomous vehicles as well as environmental, motion, and proximity sensors.

Backhaul Using Slices (Fixed Wireless Access) through commercial carriers both within and outside the U.S. to support unclassified and classified voice, data, and video traffic.

Cellular Drone Delivery/Unmanned Aerial System (UAS). Provide connectivity needed to transform UAS control from unlicensed radio to cellular, increasing security and reliability of UAS missions. Continuous Multifactor Authentication. Achieve full situational awareness to reduce uncertainty and bolster protection; includes smartphones, sensors, and security cameras.

Fixed Wireless Access (FWA) for Bases. Provide FWA as an alternative access to military bases or as redundant to existing fiber-based infrastructure.

Installation Level Micro-Grid. Optimize Marine Corps Air Station Miramar's (San Diego) micro-grid by extending the energy and water operations center to solar farms and heating, ventilation, and air conditioning networks.

Last-Mile Inport Cutter Connectivity. Coast Guard cutters require internet connectivity while moored pier side. Many current connections are copper links with low throughput. This use case would use 5G for high-speed, last-mile connectivity instead of installing fiber for each base.

Multi-Access Edge Computing (MEC) services to provide low-latency edge computing for unclassified voice, data, and video traffic.

Secure Interoperable Emergency Communications. Maintain end-to-end Quality of Service (QoS) of network slices and priority of emergency communications with the ability to differentiate whether network congestion is due to an emergency event or a cyberattack.

Single Device/Multiple Classification Levels. A National Information Assurance Partnership (NIAP)-compliant smartphone/tablet with built-in network slice selection capability to support classified and unclassified communications.

Tactical Edge Communication System. Standalone mounted and dismounted systems intended to be the next generation of tactical communications that can operate in operationally contested battlespace through the use of advanced 5G technology.

Table 1 shows that just over half of the submitted use cases anticipate using the capabilities of more than one 5G usage scenario and also shows the need for security testing and secure network slicing.

Table 1. Use Case Alignment to Usage and Testing Scenarios

Use Case	eMBB	URLLC	mMTC	Testing Scenarios	
				Security	Other
Autonomous Vehicle Proving Grounds		X			
Backhaul Using Slices	X	X		X	Network Slicing
Cellular Drone Delivery/UAS		X		X	
Continuous Multifactor Authentication		X		X	
FWA for Bases	X	X		X	
Installation-Level Micro-Grid			X		
Last-Mile In-Port Cutter Connectivity	x				
Multi-Access Edge Computing	X			X	
Secure Interoperable Emergency Comms	X	X	X	X	Secure network slicing
Single Device/Multiple Classification Levels	X	X		X	Selectable slicing, device-to-device comms
Tactical Edge Communication System	X	X	X	X	

Two use cases involve only smartphones/tablets; the remainder anticipate using more than one type of user equipment (UE) such as sensors, actuators, cameras, autonomous vehicles, UAV, and AR/VR headsets. The environment of use spans indoor, outdoor, urban/suburban/rural, and any weather or terrain. There is also a wide range in the size of the area of operation—from one square mile to the entire U.S., and the expected number of connected devices ranges from <20 per base to ≤10M across the U.S.

Table 2 below summarizes the requirements for the use cases submitted by members of the WG:

Table 2. 5G and MNI WG Use Case Requirements

Requirements	Desired Value
Autonomous Vehicle Proving Grounds	
Environment	Outdoor, indoor, urban, rural, >10 Km2
Mobility	16-80 km/h
Security	Encryption, IoT security, vulnerability testing
Sensitivity	Unclassified
Spectrum	All bands
Traffic Type	Data, Video, IoT
Backhaul Using Slices	
Mobility	Fixed
Security	Slice security
Sensitivity	Unclassified, For Official Use Only (FOUO), classified
Spectrum	All bands
Traffic Type	Voice, video, data

Requirements	Desired Value
Cellular Drone Delivery/UAS	
Connection Density	10s-100s over >10 km
Environment	Any
Mobility	8-50 km/h
Security	Authentication, encryption, IoT security, vulnerability testing
Sensitivity	Unclassified to classified
Spectrum	All
Traffic Type	Video, data, IoT
Continuous Multifactor Authentication	
Mobility	0-100 km/h
Security	Authentication, encryption, IoT security, red team/vulnerability testing
Sensitivity	FOUO
Spectrum	All bands
Traffic Type	Data, IoT
Fixed Wireless Access for Bases	
Environment	Outdoor, harsh
Mobility	Fixed
Sensitivity	Unclassified
Spectrum	mmWave
Traffic Type	Voice, video, data
Installation Level Micro-Grid	
Connection Density	Testing: 10s; ideal 100s; >10 km2
Mobility	Fixed
Other	Chemical, gas, equipment, air conditioning sensors, and actuators
Security	IoT Security
Sensitivity	Unclassified
Traffic Type	Data, IoT
Last-Mile In-Port Cutter Connectivity	
Connection Density	<20/base; 1 sq. mi.
Environment	Harsh maritime; -40 to 125°; 0-100% humidity
Latency	<100ms
Mobility	Fixed: Cutter-based wireless access point; Mobile: <60 km/h
Reliability	99.99%
Security	At least DoD type III encryption; Type I Commercial Solutions for Classified if available
Sensitivity	FOUO
Spectrum	Likely mmWave
Throughput	500 Mb/s
Traffic Type	Voice, Video, Data (Enterprise Computing)

Requirements	Desired Value
Multi-Access Edge Computing	
Environment	Any
Mobility	Fixed
Security	Edge Cloud security
Requirements	Desired Value
Sensitivity	Unclassified
Spectrum	All bands
Traffic Type	Voice, Video, Data
Secure Interoperable Emergency Communications	
Connection Density	<10M across commercial provider networks
Environment	Any
Latency	Depends on application/priority level; maintain QoS of network slices E2E
Mobility	Fixed and Mobile 1-100 km/h
Other	Secure, Federated, Interoperable Network Slicing
Reliability	Depends on application/priority level; maintain QoS of network slices E2E; ≥90% call completion rate; ≥3.0 Mean Opinion Score
Security	E2E managed security and priority
Sensitivity	Unclassified and FOUO
Spectrum	All
Single Device/ Multiple Classification Levels	
Mobility	≤120 km/h
Other	Built-in network slice selection capability
Reliability	99.999%
Security	E2E; connect to Identity and Access Management; NIAP-compliant UE
Sensitivity	Unclassified and Classified
Spectrum	All
Traffic Type	Voice, Video, Data
Tactical Edge Communication System	
Availability	99.999%
Connection Density	Mounted: 150-200 concurrent; 7-10 km radius Dismounted: 48 concurrent; 1.5-2.5 km radius
Environment	Any environment, terrain, or weather
Mobility	0-100 km/h
Other	Backpack solution with mesh networking
Security	NSA Commercial Solutions for Classified; NIAP-compliant UE
Sensitivity	Secret
Spectrum	Sub-6 GHz, mmWave future
Throughput	440/40 Mbps; > 2Gbps peak
Traffic Type	Voice, Video, Data

3.2 Other Federal Use Cases

As noted above, the use cases provided by WG members represent uses for 5G in addition to the pilot projects and other federal initiatives described in Section 2. These include DoD's requests for proposals for large-scale prototyping and experimentation of 5G technologies for DSS, AR/VR, smart warehouses, and a private 5G network; the Transportation Department's work on automated driving and intelligent transportation systems; VA's exploration of 5G for healthcare; and spectrum-related efforts. 5G also can enable:

- Sensors used for critical infrastructure or environment monitoring and alerting.
- Use of additional cameras for security monitoring to capture and process high-definition video streams.
- Use of robots or UAV for search-and-rescue operations to reduce risk to personnel safety.

3.3 Use Case Characteristics

Federal agencies will use labs to explore 5G capabilities, evaluate 5G products, conduct regression testing, test security, and experiment with different use cases for their missions. The intent of collecting federal initiatives and use cases was to identify commonalities across agencies and define a framework to conduct 5G testing that builds on the capabilities available from various 5G labs and testbeds to promote use of shared testing resources. The review of initiatives and use cases discussed in Sections 2, 3.1, and indicates that federal agencies want to take advantage of many 5G features and capabilities:

- The three International Telecommunications Union-Radiocommunications Sector (ITU-R) 5G usage scenarios: eMBB, URLLC, and mMTC
- Low-, mid-, and high-band spectrum
- Network slicing
- Fixed wireless to replace or supplement wired access
- Edge computing
- Ubiquitous connectivity to support multiple device types: smartphones/tablets, UAVs/robots, autonomous vehicles, cameras, AR/VR headsets, wearables, and IoT sensors and actuators
- Network performance improvements (latency, throughput, reliability)
- Beamforming and mmWave to enhance coverage and capacity and minimize interference

Because 5G architecture is software-based and cloud native and will rely on existing 4G technology for at least the next several years, all agencies have an interest in understanding 5G vulnerabilities and threats— both those carried over from 4G and those introduced by 5G's new architecture and features. Security testing is essential for agencies to understand and assess vulnerabilities and mitigations and to address federal cybersecurity requirements. Security testing for federal use cases includes the following areas:

- Federal cybersecurity requirements (e.g., encryption, authentication)
- Adoption of Zero Trust security architectures
- Security concerns associated with 5G and legacy 3GPP known attacks
- 5G guidelines with security protocols
- IoT security
- 5G cloud and edge security
- Secure network slicing[3]
- Secure Software Defined Networking (SDN)
- Blue/Red teaming
- Vulnerability and security assessment

3 Security of the application(s) that will use network slices also needs to be tested.

4. Insights Gained from FMG Visits to 4G/5G Labs

The 5G and MNI WG visited four types of labs during its assessment of 4G/5G labs:

- **Mobile Network Operator Labs** built with carrier-grade equipment that is/will be deployed by mobile network operators.
- **Equipment Manufacturer Labs** with carrier-grade equipment used to support cellular network operators/carriers.
- **Federal Labs** established for specific purposes (e.g., inform federal telecom policy; support defense missions; conduct testing for public safety communications, spectrum, and cybersecurity). These labs use both carrier-grade equipment and open-source elements.
- **University Labs and Testbeds** designed by academic institutions to support research and experimentation on next-generation wireless technologies. Academic labs use open-source platforms and open hardware/software for basic and applied research and experimentation.

From its visits, the WG drew the conclusions described in Figure 6 about the capabilities of the different types of labs and their suitability for use by the federal government.

Mobile Network Operator Labs	Federal Labs
Internal integration labs are designed for conformance, integration, and interoperability testing for carriers' production networks and generally not available outside the carrier and its vendors. External innovation labs are for application development, technology testing, and showcasing and are open for public use, but typically on a small scale. Carriers are a source for temporary use of licensed 5G spectrum. (Agencies could also coordinate within their organization [e.g., NTIA or DISA] or with other agencies for use of Government-owned spectrum).	Option for open field outdoor testing and specific tests (e.g., security and vulnerability testing, UAVs, autonomous vehicles). Currently use LTE, with plans to upgrade to 5G in 2021/2022. Straightforward approach for federal agency testing needs aligned to lab's purpose. Have personnel to operate testbeds and conduct testing; agencies can pay for test facilities and services through interagency agreements. May be additional costs for UE and other equipment not provided by the lab.
Equipment Manufacturer Labs	**University Labs and Testbeds**
Good option for federal testing needs via purchasing or lab as a service. Equipment conforms to 3GPP standards and continues to evolve with the standards, with some proprietary implementations for product differentiation. Offer various options for renting/leasing labs or test centers or purchasing or leasing equipment to build a dedicated lab. Additional costs for dedicated lab: installation, commissioning, maintenance support, plus cost for UE. Offer testing support services such as test design, engineering, equipment setup, test execution, and reporting, as defined in a statement of work.	Option for outdoor campus testing, use case conceptualization, and mid- to long-term R&D. Typically leverage open source technology for cost, tuning, and programmability. Designed for experimentation and exploration of new/emerging wireless technologies; generally not suited for testing of real-world implementations. Some NSF PAWR efforts specialize in building mmWave antenna arrays. Some testbeds available for federal agency use. Have personnel to run and operate testing platform; researchers pay to access the testbed but are responsible for test design, testing procedures, executing/recording test results, and providing equipment not included in the testbed

Figure 6. Capabilities of Different Types of Labs and Suitability for Use by Federal Agencies

5. Framework to Conduct 5G Testing

The 5G testing framework defines the key testing components needed that can meet the diverse needs of federal agencies. It helps 5G program managers or test managers understand the test elements and, using an example decision process, demonstrates how a test manager would determine which test elements are needed for their use case. The framework includes:

- An end-to-end 5G testing architecture and mapping to 3GPP 5G Standards.
- A high-level testing capabilities decision process to determine testing resources and budget.
- A 5G testing framework that:
  - Applies a modular approach, listing all possible elements within the framework— architecture, network, spectrum, applications, propagation, network slicing capability, and MEC—to conduct testing for different use cases.
  - Because not all elements are required for testing, articulates the capabilities of elements so only required elements are chosen for testing a particular use case.
  - Provides two examples for how to apply the framework to identify needed test elements: AR/VR and drone.
  - Addresses gaps that cannot be accomplished by the surveyed 5G labs but must be addressed in a 5G testbed.

The following is an example of how a 5G program manager can utilize the framework described in this section to build a testbed.

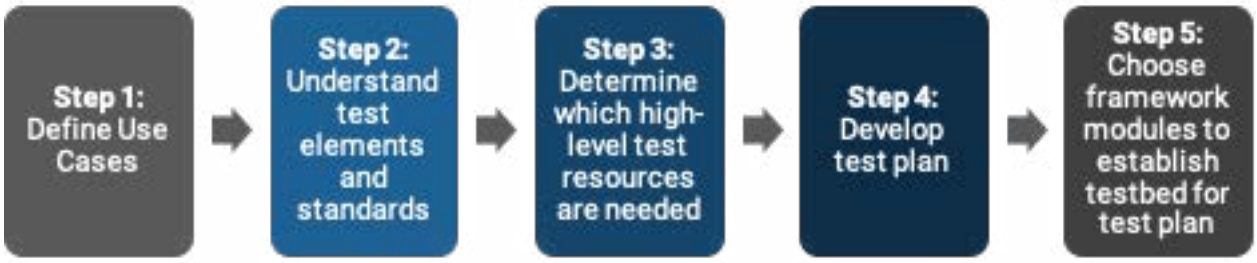


Figure 7. How to Use the Framework to Build a Test Capability

- **Step 1:** Document 5G use cases to be supported and their corresponding 5G capabilities / requirements. Refer to Sections 2 and 3 for descriptions of 5G federal use cases.
- **Step 2:** Review section 5.1 to get a general understanding of the major elements and their corresponding 5G standards to establish a 5G testbed. Review section 5.2 to understand if there are 5G testbeds offered by industry / federal agencies that can be leveraged.
- **Step 3:** From the 5G capabilities / requirements documented in Step 1 and the timeline to establish the testbed and the available budget, assess which high-level 5G testing resources are needed. There are two examples in section 5.3 "5G High-Level Testing Capabilities Decision Process". After the 5G testing resources are determined, choose a phase of the 5G testing architecture (Section 5.1.2) as your organization's 5G testbed architecture.
- **Step 4:** Develop a testing plan with test cases where each test case has an objective, testing approach, and measurements / metrics to be collected. Use section 5.2 for the factors to be considered during 5G testing to support the development of a testing plan.
- **Step 5:** Choose the modules in section 5.4 to support establishing the 5G testbed.

5.1 End-to-End 5G Testing Architecture

The main elements of the 5G network are the user equipment, RAN, edge, and core, as shown in Figure 8. The framework will support this architecture to the extent feasible to provide the end-to-end testing needed for different use cases.

Articulation of the architecture begins with a mapping of 3GPP 5G standards[4] to the 5G testing architecture followed by a phased approach to build a 5G testbed.

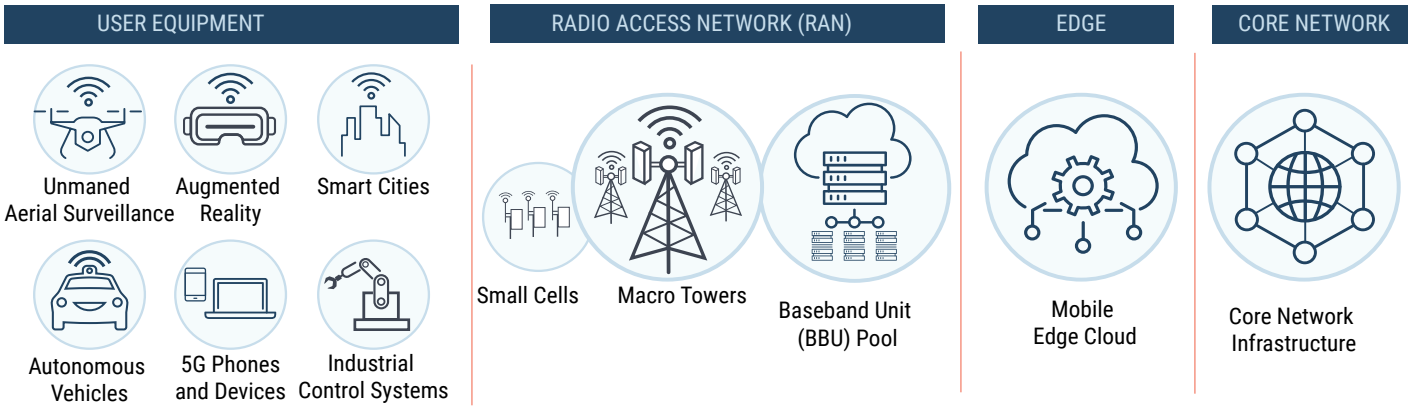


Figure 8. Major Components of a 5G Network

5.1.1 Mapping of 3GPP 5G Standards to 5G Testing Architecture

A diagram of the end-to-end (E2E) architecture with mapping of 3GPP and 5G specifications for different

Figure 9. Mapping of 3GPP 5G Specifications to 5G Testing Architecture

4 Standards for 5G are developed by multiple organizations. The European Telecommunications Standards Institute, the Global System for Mobile Communications Association, and the Internet Engineering Task Force are among the standards organizations developing 5G specifications that are used in 3GPP's specifications for 5G

components and features (UE, RAN, core, transport, and security) is shown in Figure 9 on the preceding page as reference for potential testbed designers.[5] The testing framework architecture is agnostic to 3GPP releases. Technical specifications are updated for each new release; the latest 3GPP technical specifications are in R-16. Understanding the requirements articulated in the specifications enables testing of the technologies against those requirements, including the ability to identify gaps in vendor implementations of the standards.

Table 3 below lists the key specifications for the 5G core as an example of how 3GPP standards map to the architecture.

Table 3. 3GPP 5G Core Standards

Standard	Title	Topic Areas
23.003	Numbering, addressing and identification	Including Subscription Permanent Identifier (SUPI), Subscription Concealed Identifier (SUCI), and 5G Globally Unique Temporary Identifier (GUTI) format
23.122	Non-Access Stratum (NAS) functions related to mobile station in idle mode	Definition of limited service state
23.501	System Architecture for 5G System, Stage 2	Including network slicing procedure
23.502	Procedures for the 5G System	Call flows including attach and Protocol Data Unit session establishment, network function, slice, and slice instance, network function service discovery, subscriber, and registration.
23.503	Policy and Charging Control Framework for the 5G Systems; Stage 2	
24.501	NAS Protocol for 5G System, Stage 3	UE registration with requested Network Slice Selection Assistance Information (NSSAI)
24.526	UE Policy for 5G System	How traffic is routed to UE
29.573	5G System, public land mobile network (PLMN) Interconnection; Stage 3	Security Edge Protection Proxy (SEPP) N32 interface requirements
33.401	3GPP System Architecture Evolution Security Architecture	5G Non-standalone (NSA) Security Specification
33.501*	Security Architecture and Procedures for 5G System	5G security requirements
33.511-519	Security Assurance Specifications for next- generation node B (gNB), Access and Mobility Management Function (AMF), User Plane Function (UPF), Unified Data Management (UDM), Session Management Function (SMF), Authentication Server Function (AUSF), Network Repository Function (NRF),and Network Exposure Function (NEF)	Functional conformance testing for 5G security requirements
33.535	Authentication and key management for applications based on 3GPP credential in 5G	Security features and mechanisms to support authentication and key management

**Technical specification (TS) 33.501 is the most important standard for 5G security.*

5 See also Appendix C for a list of the technical specifications articulated in Figure 9.

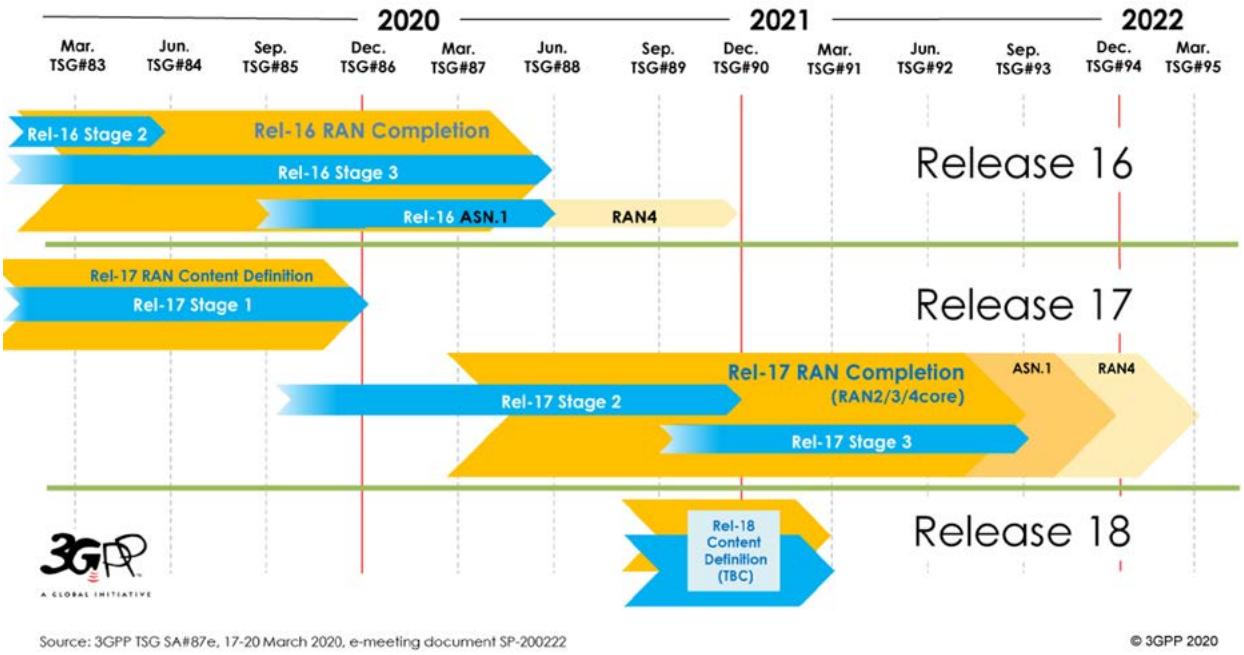


Figure 10. 5G Standards Development Timeline

5.1.2 Phases of End-to-End 5G Testing Architecture

The 5G E2E testing architecture can be divided into four main phases notionally based on the timeline for 3GPP 5G standards releases (shown in Figure 10) and 5G equipment/device vendor offerings.

The following list expands on the phases of the 5G testing architecture. The elements in Phases 1 – 4 can be carrier-grade, open source or emulated depending on the testing objectives, as long as the elements conform to 3GPP 5G specifications.

- **Phase 1:** 5G evolved packet core (EPC) with NSA option 3x deployment (3GPP R-15) including high-band (mmWave), mid-band (3.5 gigahertz [GHz] and 2.5 GHz), and low-band (600 MHz). For the NSA deployment option, each 5G gNB must be paired with an anchor 4G-evolved node B (eNB). 4G and 5G DSS 5G capability can be added in this phase.
- **Phase 2:** 5G core with SA option 2 deployment (3GPP R-15). The Phase 1 5G EPC is upgraded (software upgrade) to the Phase 2 5G core. Dual mode core (5G EPC and 5G Phase 2 core) should be considered since this is the industry trend. All gNBs deployed in Phase 1 are reusable in Phase 2.
- **Phase 3:** 5G innovations such as network slicing, distributed cloud infrastructure with cloud orchestration function, and MEC (3GPP R-15 and R-16). MEC elements must be modular and can be added to the testbed on demand.
- **Phase 4:** 5G URLCC (mission-critical communication) and massive IoT capabilities (3GPP releases 15, 16 and 17). Add to-be-determined 5G IoT devices as they become available. 5G IoT services will not be rolled out until 2022.

Following are two options for open source/open interfaces for the RAN in any phase:[6]

- **Option 1:** O-RAN5 enables 5G base stations with open interfaces. Supported by a radio intelligent controller (RIC), O-RAN enables enhanced 5G services and reduces capital expenditure.
- **Option 2:** Open-source RAN, which significantly reduces capital expenditure since RAN source code is provided by the open-source community.

An organization does not need to build or invest in all testbed phases. Rather, an organization can build a testbed for any phase(s) based on the requirements of its use cases. For example, if AR/VR support is required, there is no need to invest in/implement Phase 1 since a 5G SA core (Phase 2) is required. Table 4 below provides a timeline and summary of the use cases that can be tested in each phase.

Table 4. Timeline for Framework Phases

Phase	Timeline	Main Use Cases Supported
1	Q2 2020	FWA, eMBB
2	Q4 2020	Phase 1 + Security
3	Q1 2021	Phase 2 + differentiated QoS / priority services
4	Q1 2022	Phase 3 + Mission critical communication/URLLC, vehicle-to-vehicle (V2V), Massive IoT
Option 1	Q3 2021	Supplement any of the above phases with O-RAN
Option 2	Q4 2020	Supplement any of the above phases with Open-Source RAN

Except where noted, all modular elements discussed in Section 5.4 can be used in any of the testbed phases. The federal government also can leverage testbeds that support interconnection with other testbeds for specific use cases and/or to support security testing across testbeds that use different combinations of vendor equipment and open interfaces.

5.2 5G Testing Considerations as a Guide

When considering how to leverage capabilities of the FMG-visited labs, following are some factors to consider for testing:

- Does the lab support both 4G and 5G or just 5G?
- Is cell tower infrastructure and site support such as front, mid and backhaul (fiber), AC power, remote radio head required?
- Does the lab support vRAN, cloud RAN, and Common Public Radio Interface front haul?
- Is an RF propagation tool required?
- What application gear is provided by the lab: e.g., 5G-enabled AR/VR headsets and software?
- What application plug-ins are provided with the 5G test infrastructure?
- Is an AI platform provided to run all of the analysis and simulations?
- Is MEC required? If so, what security protections are needed at the edge?
- Is SDN/Network Function Virtualization (NFV) required?
- What IT security infrastructure (e.g., proxies, firewalls, network address translation) is required?
- Should testing include only features that will be implemented by vendors?

6 Following is a brief summary of vRAN, OpenRAN and O-RAN:
vRAN is an implementation of the RAN in a more open and flexible architecture that virtualizes network functions in software platforms based on general purpose processors. OpenRAN – disaggregated RAN functionality built using open interface specifications between elements. Can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards.
O-RAN – refers to the O-RAN Alliance or its designated specification. The O-RAN Alliance is a specification group defining next generation RAN infrastructures, empowered by principles of intelligence and openness.

- What 5G security protections does the testbed include? Do the security protections account for those included in the standards or beyond the standards such as protections against man-in-the- middle (MitM) attacks, spoofing, eavesdropping, replay attacks, DDoS, and end-to-end network slicing security?
- Does the lab have dedicated network infrastructure, shared network infrastructure, or cloud service infrastructure?
- What essential testing capabilities for chipsets, UE, RAN, core, transport, and security including E2E network slicing are needed? For security testing of UE baseband chipsets, should testing of the chipset be integrated with the UE or integrated with the RAN and core?
- What type of testing can realistically be run in the short-term? For example, network slicing cannot be tested yet. What can be modelled and what can be lab- or field-tested?
- Does testing require real or emulated base stations and real or emulated UE?
- Does the testbed need to support testing of Sub-6 GHz versus mmWave?
- Does the testbed need to provide all layers, including physical, medium access control (MAC), and higher layers or just the physical layer?
- Does the testbed provide applications or do users need to bring their own applications?
- Regarding the use of open-source (open air interface, open core, O-RAN, Open Network Automation Platform, etc.) versus carrier grade equipment for testing: Can open-source mimic a real-world 5G end-to-end environment in terms of security risk and latency performance?

5.3 5G High-Level Testing Capabilities Decision Process

This section provides a high-level decision process to assist federal 5G program managers in understanding the testing schedule (e.g., if MEC is required, it is Phase 3 of the testbed) and resource requirements. The AR/VR and drone use cases are used as examples of using the process to determine test elements needed. Both use cases fall under the URLLC usage scenario.

5.3.1 AR/VR Use Case

Step 1: Start with the use case

- AR/VR on a base

Step 2: Collect the requirements for testing scenarios.

- AR/VR requires high-data rates with low latency for end-to-end connectivity, so it needs 5G SA mode support with URLLC feature. (5G SA mode also is needed if 5G security enhancements are required.)
- There is no constraint on spectrum requirements.
- Both indoor and outdoor testing are feasible.
- One base station would suffice.
- AR/VR gear is needed.[7]6

Step 3: Map the requirements to the capabilities in the testing framework.

I. Capabilities

- Specify performance requirements in terms of:
  - Data rate
  - Latency
  - Reliability
- Performance metrics to be collected
- Identify security requirements and security metrics to be collected

7 Quality of Experience varies based on the type of AR or VR application.

II. **Architecture**
   - 5G standalone

III. **Spectrum**
   - Sub-3GHz
   - Sub-6GHz
   - mmWave
   - CBRS (Note: CBRS currently does not support 5G)

IV. **Testing resources required**
   - Environment of use/area: Specify whether environment is indoor or outdoor
   - Specify size of area of operation and whether it is urban, suburban or rural
   - Specify network size
   - Number of 5G base stations: One
   - Type/number of mobile devices: AR/VR headsets
   - Traffic type: Video, data
   - Project traffic volume (bandwidth and number of simultaneous connections)
   - Communication interaction: Human to Machine
   - 5G innovation capabilities:
     - Network slicing to support traffic priority differentiation
     - MEC to enable low-latency applications
     - Security classification: Unclassified, FOUO

Figure 11 below is a sample design that maps the AR/VR use case to the capabilities in the testing framework (Step 3 in Figure 7).

Figure 11. Result of Step 3 for AR/VR Use Case

Step 4: Develop a testing plan with test cases that include test objective, testing approach, and measurements to be collected.

Step 5: What existing capabilities/resources can be leveraged (national laboratory, university, DoD, spectrum from carriers)? Not everything needs to be built from scratch by purchasing/leasing equipment. For example, carrier-grade equipment vendors can offer 4G/5G base stations as well as a 4G/5G core.

Federal labs can offer testing chamber(s), testing equipment (e.g., spectrum analyzer and protocol analyzer), emulation equipment, and outdoor testing venues. University labs can offer testing equipment, emulation equipment, and campus testing venues. 5G cellular network operators or other agencies can offer licensed spectrum. In addition, there are initiatives that interconnect different 5G labs that also can be leveraged.

5.3.2 Drone Use Case

Step 1: Start with the use case

- Drone near the border

Step 2: Collect the requirements for testing scenarios.

- A drone requires high-data rates with low latency for end-to-end connectivity, so 5G SA mode support with URLLC feature is required. (Note: If there are many drones, massive IoT features are also required.)
- There is a constraint on spectrum because drones operate outdoors and require spectrum coordination.
- Only outdoor testing is feasible.
- Multiple base stations are required.
- Drone is needed.
- If 5G security enhancements are required, a 5G SA mode is needed.

Step 3: Map the requirements to the capabilities in the testing framework.

I. Capabilities

- Specify performance requirements in terms of:
  - Data rate
  - Latency
  - Reliability
  - Mobility
- Performance metrics to be collected
- Identify security requirements and security metrics to be collected

II. Architecture

- 5G standalone

III. Spectrum

- Sub-3GHz
- CBRS (note that CBRS currently does not support 5G)

IV. Testing resources required

- Environment of use/area: rural, uneven terrain, possibly contested
- Specify size of area of operation
- Specify network size
- Number of 5G base stations: Multiple
- Type/number of mobile devices: Smartphone/tablet and drones/IoT
- Traffic type: Video, data
- Project traffic volume (bandwidth and number of simultaneous connections)
- Communication interaction: Human to Machine and Machine to Machine
- 5G innovation capabilities:
  - Network slicing to support traffic priority differentiation
  - MEC to enable low-latency applications
  - Security classification: Unclassified, FOUO, Classified

Step 4: Develop a testing plan with test cases that include test objective, testing approach, and measurements to be collected.

Step 5: What existing capabilities/resources can be leveraged: national laboratory, university, DoD, spectrum from carriers? See AR/VR subsection. Some federal labs have air space for UAV testing.

5.4 Modular Elements for the Framework to Conduct 5G Testing

The modular elements needed for the 5G testing framework are discussed below. The modules are organized by architecture, spectrum, application traffic, network, and 5G innovations. Each subsection includes a description and considerations for the test element as well as associated test and measurement equipment (e.g., spectrum analyzer, protocol analyzer, and signal generator). Not all elements are required for testing. The elements required to support various use cases are summarized in Table 5 below.

Table 5. Modular Elements Required for Different Use Cases

Modular Element	Use Case
Section 5.4.1: Architecture	
NSA (5.4.1)	FWA, eMBB
SA (5.4.1)	URLLC, massive IoT, security
Section 5.4.2: Spectrum	
Channel Emulation (5.4.2.2)	Required when outdoor testing or mobility cannot be supported
Cabled Testing (5.4.2.4)	Sub-6 GHz (required when over-the-air testing cannot be supported)
RF Chamber (5.4.2.4)	Sub-6 GHz (required when over-the-air testing cannot be supported)
Anechoic Chamber (5.4.2.4)	mmWave (required when over-the-air testing cannot be supported)
Spectrum Analyzer (5.4.2.5)	All except security
Section 5.4.3: Application Traffic Generation	
Application Traffic Generation	All
Section 5.4.4: Network	
Indoor (5.5.4.1)	eMBB, security
Outdoor (5.5.4.1)	FWA, URLLC, massive IoT
Emulated UE (5.4.4.2)	URLCC, massive IoT (if required number of real UEs is not sufficient)
Emulated Core (5.4.4.3)	All (required when isolation of core elements is required)
Emulated RAN (5.4.4.4)	All (required when real RAN is not available)
Signal Generation (5.4.4.5)	All (required when interference is required)
Protocol Analyzer (5.4.4.6.1)	All

5.4.1 Architecture (LTE, 5G NSA, 5G SA)

Some use cases (see Table 5 above) may need to leverage the LTE architecture to support compatibility and regression testing. To test any 5G security features, end-to-end network slicing, and MEC, the testbed must support the 5G standalone (SA) architecture.

5.4.2 Spectrum

There are differences in antennas, testing equipment, and test methods used to generate, test, and analyze mmWave spectrum and sub-6 GHz spectrum that need to be accommodated in a testbed.

5.4.2.1 Antennas (Panel Antenna/Antenna Array)

For 4G eNBs used in NSA mode or 5G gNBs supporting Sub-3 GHz, panel antennas are typically used; while 5G gNBs supporting mmWave and Sub-6 GHz (but above Sub-3 GHz) typically use antenna arrays.

5.4.2.2 Channel Emulation

Channel emulation hardware equipment is required for sub-6 GHz to account for in-building penetration and various types of propagation environments such as line of sight (LoS), non-LoS, blockage, and reflection due to terrain and fading effects to support testing in a cabled environment. Channel emulation models typically support various morphologies (rural, urban and suburban), indoor, macro cells, microcells, buildings and their densities, trees and their densities, and water.

However, mmWave channel emulation requires consideration of its beamforming effects, which introduce angle-of-departure and angle-of-arrival geometry into the channel calculations. 3GPP TR 38.901, "Study on channel model for frequencies from 0.5 to 100 GHz" specifies channel models for:

- Urban Macro
- Urban Micro
- Indoor
- Others

5.4.2.3 Fading Considerations Due to Mobility

Mobility introduces fast fading and doppler effects into cellular communications. For use cases with mobility requirements (pedestrian, vehicular, drones), the testing must be done either outdoors (for vehicular or drones) or indoors with a propagation channel emulator.

5.4.2.4 Cabled Testing vs. RF Chamber vs. Anechoic Chamber

Sub-6 GHz testing can be done using cabled testing or over-the-air. The number of RF channels and the level of component integration in mmWave antenna arrays makes it impractical to conduct testing by connecting an mmWave device to the test equipment with cables. Thus, mmWave testing needs to be done over-the-air inside an anechoic chamber.

5.4.2.5 Spectrum/Signal Analyzers

Typical spectrum analyzers work from 30 MHz to 6 GHz; with an upgrade, an analyzer can work from 6 GHz to the mmWave frequency range. A spectrum analyzer offers the following basic capabilities: phase noise level; intermodulation suppression and out-of-band measurements including adjacent channel leakage ratio and spectrum emission mask measurements; and harmonic measurements.

A spectrum analyzer may offer the following advanced capabilities:

- Support for all specified 5G signal bandwidths—from 5 MHz to 400 MHz—with multiple numerologies, multiple bandwidth parts, and modulation formats from Quadrature Phase Shift Keying to 256 Quadrature Amplitude Modulation.
- In-band measurements of 3GPP 5G NR in the downlink (DL) and uplink (UL). Each signal subframe is analyzed as well as a wide range on a per-subframe basis.
- Provide measurement results for error vector magnitude, frequency, and power of different channels and signals.

5.4.3 Application Traffic Generation

Application traffic can be live or emulated. The following tools/methods can be used to generate emulated application traffic:

- iPerf (a free software tool https://iperf.fr/).
- Use/acquire hardware from a testing vendor that supports various types of applications and produces assessments of video, data, and voice quality.
- Generate real or emulated application traffic from multiple UEs.

5.4.4 Network

5.4.4.1 Indoor or Outdoor

Whether testing should be conducted indoors or outdoors should be dictated by the use case, e.g., if the testing involves UAVs or autonomous vehicles, outdoor testing is essential due to the nature of how the devices are used. However, security testing can be done indoors or outdoors. A federal lab's outdoor test range can be leveraged for outdoor testing. Some university labs also offer outdoor campus or city-scale testing. All federal and academic 5G labs have indoor testing capabilities.

5.4.4.2 Real UEs and Emulated UEs

For real UEs and emulated UEs, testing may be radiated (tested over the air) or conducted/cabled (by connecting UEs to a base station via cables). For use cases that require only a few UEs, real UEs are adequate. However, if the use case requires hundreds or thousands of UEs, emulated UE equipment is needed. The issue with emulated UEs is that they all share the same high-power amplifier on the test equipment, so power control may not work effectively. As a result, emulated UEs are adequate to provide background traffic to test use cases such as priority services under overload conditions. Emulated UEs are able to support all 5G spectrum bands that conform to 3GPP 5G protocols and for load testing.

Another advanced capability for 5G UEs is the number of slices supported simultaneously. The 5G standard allows eight simultaneous slices per UE, however, no current commercially available UEs support this feature.

5.4.4.3 Real Core and Emulated Core

Core network emulators (from a testing vendor) provide simulated user plane and control plane protocol traffic and provide the capability of isolating the gNB under test to enable testing the gNB from "both sides". This type of emulated core is also treated as a black box and only the interfaces serving the RAN are exposed. Some of the reasons to use an emulated core for testing are:

- A core is not available due to lack of resources.
- A core is available as a shared resource in a test environment but is being used by another testing customer.
- A core is available, but the overall test program intentionally segregates the testing for RAN and core to verify each independently before integrating them for end-to-end testing.

Core network emulators also can emulate the effects of many UEs and base stations. They are scalable, with the limit set by the compute resource the emulator is built upon. Typically, emulated UEs and base stations are "soft" (i.e., they cannot radiate over the air) and are simply created to generate traffic load in both the user plane and control plane. The "soft" UEs and base stations can emulate the data network and user plane function by generating voice, data, and video traffic and also can test reliability and capacity of the network. Some vendors also can insert malware and simulate denial-of-service (DoS) attacks to test vulnerabilities in the core.

Core network testers can emulate certain elements of the core and isolate those elements; these testers can also emulate one or more of the core's microservices, which could compose a complete ecosystem with all interfaces exposed.

Advantages of black box core emulation include:

- Only the interfaces to the RAN are exposed. This simplifies the task of configuring, testing, and troubleshooting.
- It also can run as a virtual function, which reduces the lab footprint.

Its disadvantages include:

- Design for a core emulator follows 3GPP specifications. However, carrier-grade core network vendors add proprietary features to differentiate their products. It is difficult for core emulator vendors to incorporate those features into their products.
- Support for the latest 3GPP specifications may lag behind carrier-grade core network vendors.

5.4.4.4 Real gNB and Emulated gNB

The RAN is an essential element of a 5G network. There are two mechanisms to deploy a RAN node (e.g., gNB) in 5G NSA or SA networks: real gNB from a 5G equipment vendor or emulated gNB from a 5G testing vendor. In general, the emulated gNB is designed to support conformance testing of UEs.

Almost all testing vendors support the testing of only one UE at a time. A separate remote radio head (RRH)[8] for mmWave spectrum testing may be required. The core network functionality is greatly simplified inside the emulated gNB. In general, emulated gNBs are more expensive than real gNBs since emulated gNBs include additional features such as scripting or testing cases and the flexibility to modify over-the-air messaging content.

5.4.4.4.1 O-RAN gNB

Most O-RAN testing capabilities are the same as those for emulated gNB (see https://www.o-ran.org/ for O-RAN vendors). O-RAN testing capabilities that are unique to O-RAN include:

- Test vectors for Control, User, and Synchronization Plane
- Emulate O-RAN Distributed Units (O-DUs)
- Analyze O-RAN Radio Unit (O-RU) responses
- Compliance testing for O-RU for operation and radio performance

5.4.4.5 Signal Generation Including Interference Signal

A signal generator is required to create signals for testing, including interference, to verify, for example, the co-existence of multiple types of signals. The types of interference include unintentional interference, coexisting interference (e.g., with radar), or intentional interference (e.g., jamming). A signal generator has the following basic capabilities:

- Frequency range from 100 kHz to 6 GHz or above (to mmWave frequency).
- In-phase and quadrature (IQ) modulation bandwidth in the GHz range.
- Supports important digital communication standards including 5G NR, LTE, etc.
- Optionally can include a fading emulator (see section 5.4.2.3).
- Supports all key multiple-input, multiple-output (MIMO) modes.
- Supports 3GPP conformance testing standards.

Advanced 5G signal generation capabilities include:

- UL and DL 5G NR signal generation that supports multiple waveforms, channel bandwidths, modulation schemes, and numerology options specified in the 3GPP standards.
- Configuration of additional parameters, e.g., bandwidth parts and resource allocations.

5.4.4.6 Coverage Testing

Drive/walk testing throughout the area of interest with a protocol analyzer is required to understand the gNB quality of coverage for UEs. The following are metrics of interest for coverage testing:

- Random Access Channel (RACH) information
- Transmit power
- Rank (MIMO mode)
- Modulation
- MAC throughput and block error rate (BLER)
- Signal strength
- Quality metrics of the Synchronization Signal Block (SSB) beams
- QoS measurements: throughput and latency

8 Emulation of mmWave would not be accurate to what would be seen in the field unless the emulator uses the same radio head and beamforming mechanisms as commercial vendors.

5.4.4.6.1 Protocol Analyzers

There are two types of protocol analyzers: UE-based and recorder-based. Both types provide collection and analysis capabilities:

- UE-based protocol analyzers require the use of a 5G UE to connect to a 5G network; the analyzer obtains all metrics and statistics of the 5G connections via the 5G UE. If the 5G UE is connected to a 5G network from a service provider, a Subscriber Identity Module (SIM) card with an active subscription is required.
- Recorder-based protocol analyzers do not need to connect to 5G UE. These analyzers store all the IQ signals of 5G connections (from many UE) for a particular frequency channel. The analyzer then processes the IQ signals and applies decoding to discover all 5G connections. The advantage of this type of analyzer is it provides a global view of all the 5G connections, which is difficult to achieve using a UE-based protocol analyzer. A drawback of this type of analyzer is that after authentication is completed, many layer 2/layer 3 messages are encrypted. As a result, it becomes difficult to troubleshoot the network.
- Figure 12 below is a capture from a protocol analyzer for a 5G mmWave network. The highlighted rows show that there are multiple beams per 5G NR cell (four have been identified by the protocol analyzer) and that throughput reaches 1.8 Gbps.

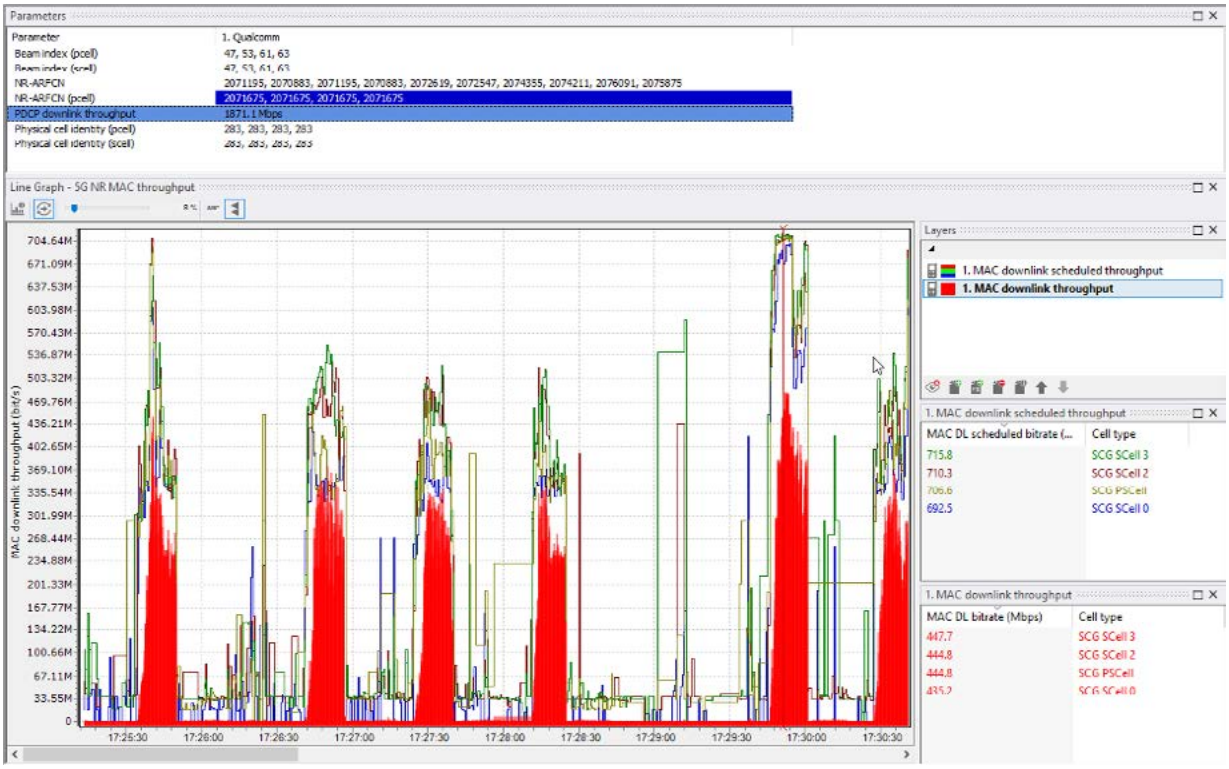


Figure 12. Protocol Analyzer Capture for 5G NR mmWave Cell*

**NR-ARFCN: New Radio Absolute Radio-Frequency Channel Number*

5.4.4.7 Timing and Synchronization

The testbed needs to support timing and synch emulation with features emulating packet loss and loss of synchronization.

5.4.4.8 Transport Layer

The testbed also needs to support an Ethernet IP test solution and fronthaul/backhaul testing.

5.4.4.9 5G System Simulator

A 5G system simulator is one possible approach to evaluate the performance of a 5G system using modeling and simulation techniques. A 5G system simulator abstracts the behaviors of each element in a 5G system with a simplified protocol stack/calling ladder as well as a simplified physical layer. It can provide outputs in data rate and bit error rate given signal-to-interference-plus-noise ratio and channel bandwidth, for example.

Advantages of a 5G system simulator include affordability and ease of scaling to simulate a large 5G system with many RAN nodes and UEs. However, a 5G system simulator lacks performance fidelity compared to a 5G system with real elements provided by 5G infrastructure vendors. A 5G system simulator is typically used by universities to conduct academic research, not to evaluate the performance of real 5G networks. For best results, the performance of real 5G networks should be evaluated using real 5G systems.

5.4.5 Performance Metrics That Can Be Collected

Following is a summary of the performance indicators and performance metrics that can be collected on a 5G testbed:

- Quality of service (E2E latency for data plane, E2E latency for control plane, jitter, data rate/throughput, packet success rate).
- Quality of experience (QoS retainability, service continuity (%), mobility interruption time, availability).
- UE metrics:
  - Battery life, battery aging
  - Quality of service (block error rate, sensitivity)
  - Throughput
  - Latency
- Network slice performance metrics:
  - E2E latency through a slice
  - Average bandwidth allocated to a slice

5.4.5.1 AI/ML Platform for Testing and Analysis

The goal of using an AI/ML platform is to develop a ML model to perform a specific task. An AI/ML platform can automate testing, analyze and report results, as well as optimize and tune thousands of network parameters during testing; thereby reducing the amount of manual effort needed to execute tests and analyze test outputs. Similar ML models can be developed with most AI/ML platforms currently available by providing the same information from testing data as well as the testing environment. Two popular AI/ML platforms are:

- TensorFlow, created by Google, is able to leverage multiple programming languages including Python,[9] JavaScript, and Swift.
- Caffe is another popular AI/ML platform. Developed by the University of Berkeley with a community of interest, Caffe is written in C++ with a Python interface.

5.4.6 5G Innovations Considerations

5.4.6.1 Network Slicing with Orchestration

Network slicing is a modular element that can be added to the 5G testing framework. E2E network slicing includes core slice, transport slice, and RAN slice. As shown in Figure 13 below, network slicing requires orchestration and virtualization support. Due to virtualization, many network elements are cloud-based and hosted in a virtual environment instead of using dedicated hardware equipment. As a result, the testing paradigm also shifts from testing dedicated hardware to testing virtual functions and the cloud implementations to understand the problems.

9 Python is the most popular programming language for AI/ML platforms.

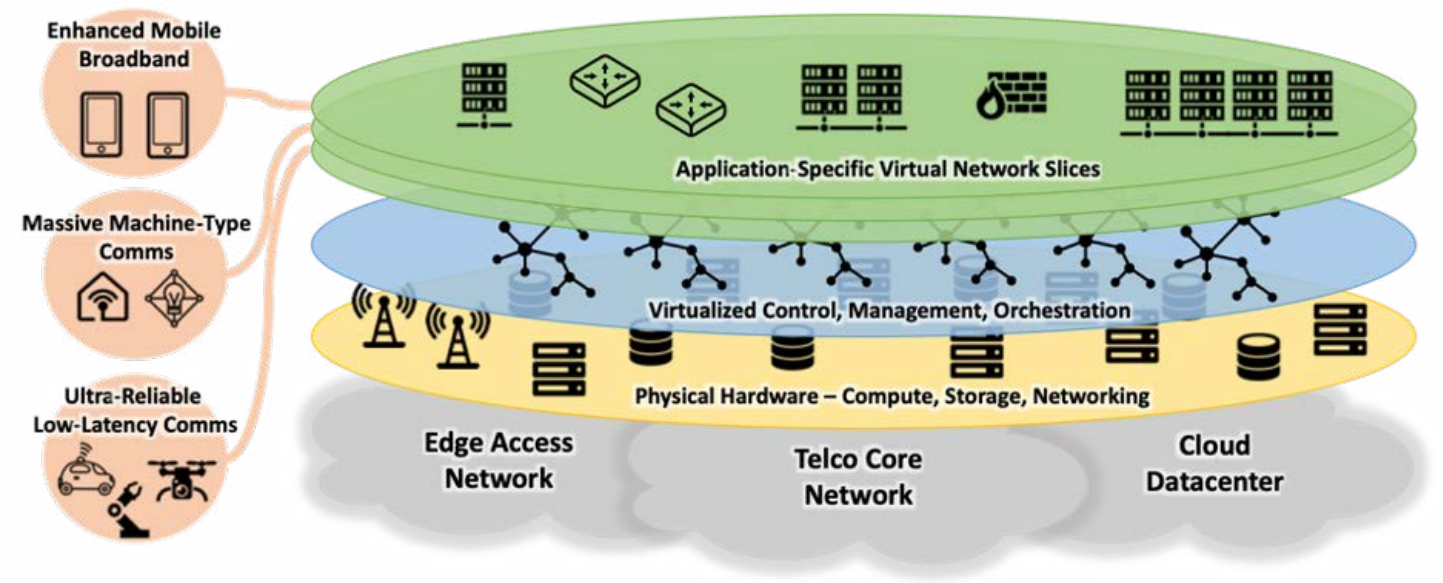


Figure 13. Network Slicing and Virtualization

The following are configurable capabilities for network slices[10] from the end-user viewpoint. The performance of these capabilities also can become testing targets:

- QoS, including data rate and latency
- Reliability
- Security
- Network services, including analytics and content enrichment

All 5G equipment vendors offer their own solutions for provisioning network slicing. Following are some considerations for network slice testing:

- Establish the baseline topology with no slice.
- Create a slice by initiating new instances of the User Plane Function (UPF) and/or Access and Mobility Management Function (AMF). UE/gNB and the data network can be simulated. The Network Slice Selection Function (NSSF) and Network Repository Function can be simulated initially to reduce cost and complexity but should migrate to real elements. The network response to a slice creation request should be tested and characterized as another baseline.
- Start with a simple test case with one UE and two slices, where each slice has its own Protocol Data Unit (PDU) and Data Network Name (DNN). Collect slice metrics for UL and DL traffic, including latency.
- Test multiple UEs with multiple PDU sessions on multiple slices; bring down one slice (e.g., unreachable DNN) and verify whether the performance of other slices has been affected.
- Test with multiple slices where one slice has excessive traffic and verify if the performance of other slices has been affected.
- Test with multiple slices with differentiated QoS (from RAN perspective) and evaluate the performance of these slices via RAN slicing.
- Test with an element isolation scenario to evaluate performance, e.g., emulate AMF or NSSF with other real elements and evaluate the real UPF and/or SMF performance with multiple slices.
- Perform negative testing with NSSF by injecting invalid requests/inputs.

10 https://www.gsma.com/newsroom/all-documents/generic-network-slice-template-v2-0/ (Link accessed July 8, 2020)

Additional topics for network slice testing are:

- The security and automation of network slicing orchestration.
- Testing the actual level of isolation of network slices in resources and security.

More research from the vendor community is required to determine how to evaluate network behavior of orchestration, which defines how and where virtual network functions (VNF) are created for slice support.

5.4.6.2 Multi-Access Edge Computing (MEC)

MEC is a feature to reduce network congestion and application latency to users by pushing the computing resources, including storage, to the edge (e.g., base stations). The edge in MEC offers application developers and content providers cloud computing capabilities and an IT service environment at the edge of the external data network.

The deployment of MEC at the network edge reduces E2E application latency and improves the user's quality of experience to enable real-time, high data rate and high reliability applications to support use cases such as video surveillance with analytics, location tracking, industrial automation, and V2V communications. To allow MEC to optimize user application performance and perform local traffic rerouting, 5G network capabilities need to be exposed to the MEC via the 5G service-based architecture (SBA) Network Exposure Function (NEF). The capabilities exposed are from the 5G core and 5G RAN. The MEC orchestrator acts as an Application Function (AF) to the 5G network.[11]

MEC is a modular element that can be added to the 5G testing framework to support testing of certain applications as discussed above. There are various MEC and 5G system interfaces that can be exposed to allow MEC to use the interfaces to provide advanced services to customers. However, the interfaces that are exposed can differ by vendor, thus a unified testing lab for MEC will be needed to compare the performance of MEC offerings from multiple vendors.

5.5 Security Considerations for the 5G Testing Framework

Table 6 below compares security features between 4G and 5G and whether the features are mandatory or optional to deploy by 5G cellular network operators. This comparison is from the viewpoint of 5G operators, not 5G equipment vendors. Note that 5G security typically implies that the security capabilities are for SA mode deployment. For NSA mode deployment, the security capabilities are essentially the same as those for 4G. However, since NSA does support 5G NR, the following 5G security capabilities are applicable for NSA: over the air transmission between UE and gNBs such as confidentiality/integrity for Non-Access Stratum (NAS) (NAS is the control plane between UE and the core network signaling); user data plane; and Radio Resource Control (RRC) (RRC is the control plane between UE and base station signaling).

Table 6. 4G / 5G Comparison of 3GPP Enhanced Security Features

5G Security	5G in R-15 (3GPP TS 33.501)	4G (3GPP TS 33.401)
NAS signaling confidentiality	Optional	Optional
NAS signaling integrity	Mandatory	Mandatory
User plane data confidentiality	Optional	Optional
User plane data integrity	Optional	Does not exist
RRC signaling confidentiality	Optional	Optional
RRC signaling integrity	Mandatory	Mandatory
UE Configured Radio Technology Restriction	Optional	Does not exist
SUPI encryption (a.k.a. SUPI/International Mobile Subscriber Identity [IMSI] privacy)	Optional (has exceptions)	Does not exist
Network security – IPSec	Optional	Optional
Core network security – TLS	Optional	Optional

11 "MEC in 5G networks." ETSI. First Edition – June 2018. Online: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf (Link accessed July 8, 2020)

5G Security	5G in R-15 (3GPP TS 33.501)	4G (3GPP TS 33.401)
Security Edge Protection Proxy (SEPP)	Mandatory	Does not exist
Key size	256 bits allowed	128 bits

The following list provides recommendations to address these gaps:

- Turn on the 5G optional security features before network deployment or conducting security tests.
- Enable user plane confidentiality and integrity as well as signaling confidentiality.
- Deploy subscriber privacy.
- Monitor exception scenarios for the Subscription Concealed Identifier to use null scheme.
- Use Internet Protocol Security (IPSec) where recommended and use Transport Layer Security (TLS) between core functions within a security domain.
- Push for the use of 3GPP Security Assurance Specification (SCAS) for various network functions in the 5G system. SCAS provides functional conformance testing for 5G security requirements.
- There is also a R-17 technical report addressing Security Assurance Methodology and SCAS for 3GPP virtualized network products.
- Outside the realm of 3GPP, mandate that vendors provide a disable legacy RAN functionality that can be controlled by both a user and an organization's mobile device management solution.

5.5.1 Security Testing

The security testing to be conducted differs based on the security domains under consideration. Each security domain includes the security capabilities defined by 3GPP 5G security standards/industry best practices. The objective of security testing is to apply potential threats against the security capabilities in a security domain to identify vulnerabilities. Testing vendors have products to emulate different levels of security threats against security domains. The following are the security domains[12]11 for 5G, with examples of potential threats in some of the domains:

- Network access security.
- Network domain security: Attacks on network-to-network interfaces with external networks such as the public switched telephone network, Internet, or non-3GPP access networks.
- UE domain security: DDoS attack from a botnet of infected mobile devices.
- Application domain security.
- SBA domain security.
- Transport security: Attack between RAN and core via third-party transport network interfaces.
- SDN/NFV security: Side channel/covert channel or third-party VNF or SDN attacks on network nodes where various network slices are co-resident; orchestrator configuration errors or malware attacks from third-party SDN attacks in core network.
- Network slicing security: Attacks generated when network slices traverse untrusted hardware or networks in the core, transport, or RAN segments.
- MEC security.
- Management security.
- IoT security: DDoS, man-in-the-middle/spoofing, malware.
- gNB security: RF noise attack and physical attack: An RF noise attack, or RF barrage jamming, occurs when an attacker deploys unauthorized radio devices to launch intentional interference to deny or downgrade communication links between 5G gNB and 5G UEs. Due to densification of cell deployments in 5G, a much larger number of unprotected/exposed small cells in dense network areas such as cities presents the threat of physical compromise of a gNB by an attacker.

12 "Keysight 5G security Overview."

Certain 5G techniques such as antenna beamforming with directivity, Multi-Radio Access Technology Dual Connectivity, and dedicated RAN slicing can be deployed as potential mitigations for RF noise attacks. Perimeter security, including intrusion detection with alarms, needs to be deployed to protect unprotected small cells in dense networks. When vRAN is introduced, gNB can be separated into distributed units (DU) and centralized units (CU). The DU is placed near the antenna and the CU, which stores sensitive information, can be placed inside a trusted and physically secure location to increase overall protection.

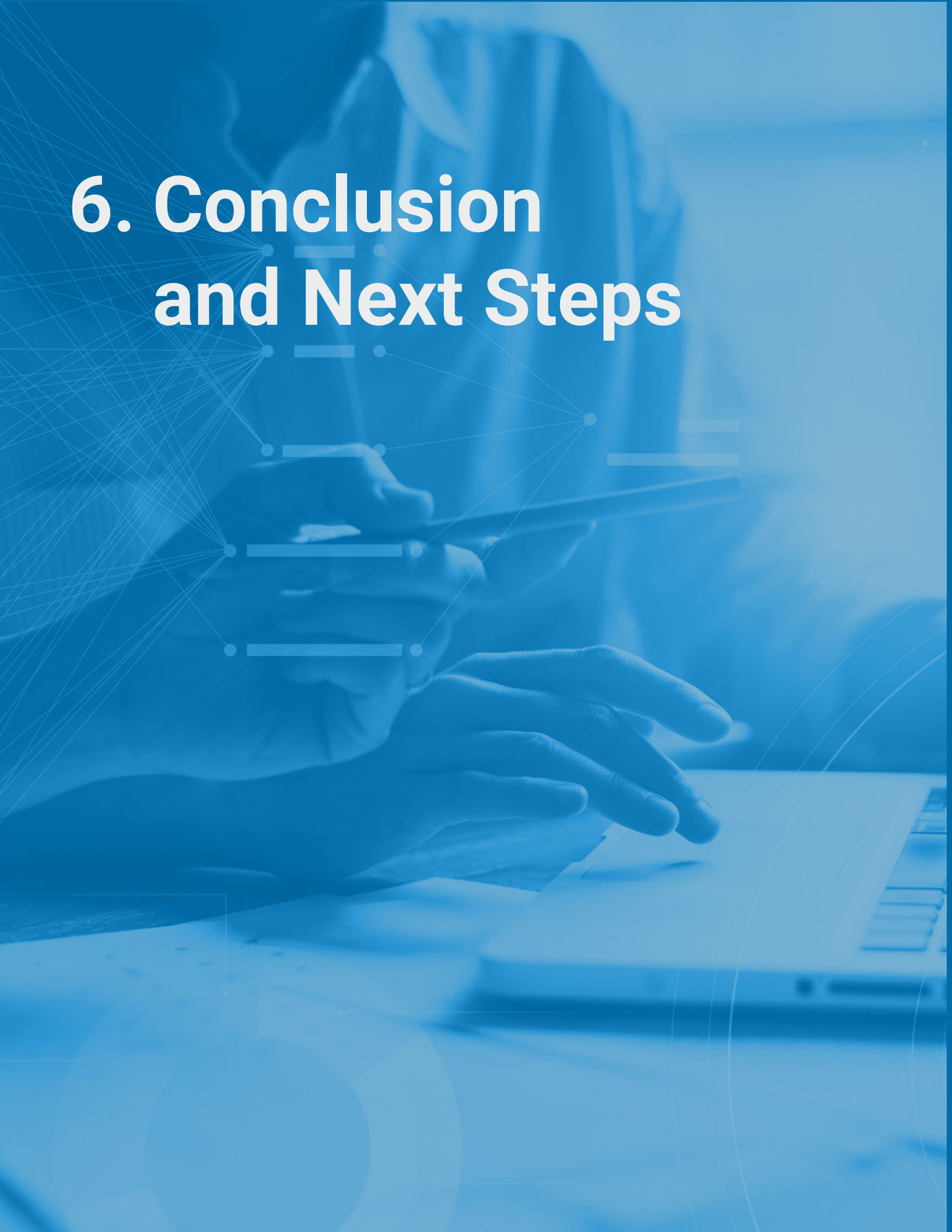
Note that security and QoS are inter-related. While conducting security testing, the impact of security controls on network performance and the ability to maintain QoS of different network slices (e.g., FWA, eMBB, URLLC, mMTC, and V2V) end-to-end across the network to support government missions should also be assessed.

Security testing vendors offer security testing packages that can generate attacks such as DDoS and malware insertion. These packages can be used to test reliability of the data network and the core network. To address federal security requirements, federal-owned or federal-sponsored security testing infrastructure for 5G will be needed. Agencies may be able to leverage DoD's 5G prototyping projects for security testing.

5.5.2 Security Metrics That Can Be Collected

Following is a summary of the security metrics that can be collected on a 5G testbed:

- Quality of security (threat identification (%), attacks prevented (%), time to identify vulnerability, time to mitigate vulnerability).
- Quality of reliability (E2E reliability, which is the meantime between failure and service restoration).
- Quality of transmission security (low probability of intercept, low probability of detection, low probability of geolocation).
- Additional security key performance indicators include:
  - Side channel/covert channel leakage (b/s)
  - Time to identify and isolate an attack
  - Time for network slice/VNF migration to a different node
  - Time for probes to identify and block attacks from untrusted hardware or network segments that a network slice may traverse.
- Network availability and reliability.



6. Conclusion and Next Steps

Federal agencies are actively seeking to take advantage of 5G's features and expanded connected services to improve mission delivery and business operations and to deliver new applications and services for employees and citizens. Agencies will use 5G labs and testbeds to explore 5G technologies, products, and services; experiment with different use cases for their missions; and examine security protections and vulnerabilities. To avoid duplication and promote use of shared testing resources, FMG's 5G and MNI WG previously surveyed a set of 4G and 5G labs and testbeds nationwide and developed conclusions regarding lab capabilities and their suitability for use by the federal government.

Equipped with information about the visited labs' existing and planned 5G test capabilities, this document refines federal use cases for 5G and defines a framework for conducting 5G testing. A review of 5G- related federal initiatives and collection of use cases submitted by members of the WG indicates that

agencies want to leverage many of 5G's enhanced and new capabilities, including:

- The 5G usage scenarios in environments that include indoor, outdoor, urban, suburban, and rural, all weather and terrains, and on the battlefield.
- The use of low-, mid-, and high-band spectrum to meet different throughput and coverage requirements.
- 5G innovations of network slicing and MEC for differentiated service and low latency.
- Deployment of multiple types of user equipment—smartphones, unmanned aerial vehicles, autonomous vehicles, cameras, AR/VR headsets, and a variety of IoT sensors and actuators.
- Ability to meet different performance requirements for latency, throughput, and reliability.
- Beamforming and mmWave to enhance coverage and capacity and minimize interference.

This framework for 5G testing identifies the modular capabilities and elements needed to conduct 5G testing. The 5G testing architecture is divided into four phases, notionally based on the timeline for 3GPP 5G standards releases and 5G equipment/device vendor offerings. The elements of the framework are organized by architecture, spectrum, application traffic, network, and 5G innovations. Each subsection includes a description and considerations for the test elements and associated testing equipment (e.g., spectrum analyzer, protocol analyzer, and signal generator). A separate section discusses security considerations.

The framework helps 5G program managers or test managers understand the test elements needed to conduct testing of their use cases. After using the framework to identify the modular elements necessary for a federal use case, a federal agency is able to choose an appropriate suitable testing resource/lab (e.g., a federal lab, university lab, or coordination with DoD) to conduct testing, to build/lease a testbed from a carrier-grade equipment manufacturer for dedicated 5G testing, or to collaborate and establish a shared resource that could include interconnected testbeds. Agencies will need to verify that existing labs/testbeds selected for their use cases include capabilities to manage and execute tests and a platform for analysis and reporting.

The framework supports activities related to collaboration and shared lab capabilities in the *National Strategy to Secure 5G Implementation Plan.* Although the framework is intended to support coordination of 5G test activities across the federal government and documents federal 5G initiatives and use cases, the process for developing the framework and defining its modular elements can be applied more broadly to both public- and private-sector enterprises. FMG is working with NITRD to determine how to leverage the framework and the testbed assessment for the shared testing activities in the *Implementation Plan*.

Appendix A Overview of 5G

The International Telecommunications Union-Radiocommunications Sector (ITU-R) defines the requirements and capabilities for third generation (3G), 4G, and 5G as well as their performance indicators (e.g., latency, data rate). The ITU's International Mobile Telecommunications Vision 2020 defines three usage scenarios for 5G that distinguish 5G from 4G telecommunications. Depicted in Figure 14 and frequently referred to as the "5G triangle", the scenarios are:[13]

- **Enhanced mobile broadband (eMBB)**, which primarily focuses on higher data rates with a peak data rate improvement from 4G's one Gbit/s to 20 Gbit/s.
- **Ultra-reliable, low-latency communications (URLLC)**, also called **critical machine-type communications**, is a new usage category that requires enhanced capabilities for high reliability, low latency (as low as 1 ms), and high mobility (up to 500 km per hour).
- **Massive machine-type communications (mMTC) or massive Internet of Things (mIoT)** is intended to serve extremely high-density deployments of low-complexity, low-power consumption IoT devices (one million devices in a square kilometer) transmitting low volumes of non-delay-sensitive data.

Figure 14. 5G Usage Scenarios

13 Recommendation ITU-R M.2083-0. "IMT Vision – Framework and overall objectives of the future deployment of IMT for 2020 and beyond." International Telecommunications Union. September 2015. Online: https://www.itu.int/rec/R-REC-M.2083- 0-201509-I/en (Link accessed May 15, 2020)

A.1 Capability Enhancements for 5G

Meeting the objectives for 5G will require significant capability enhancements in terms of higher data rates, reduced latency for critical communications, ability to support the increased number of connected devices, higher mobility, and spectrum availability as shown in Table 7.

Table 7. . Capability Improvements from 4G to 5G

Key Capability	4G	5G
Peak data rate (Gbits/s)	1	20
User experienced data rate (Mbits/s)	10	100
Relative spectrum efficiency	1x	3x
Mobility (km/h)	350	500
Latency (ms)	10	4 (eMBB); 1 (URLLC)
Connection Density (devices/km2)	100,000	1 million

Understanding the capability enhancements will help agencies determine whether their envisioned use cases require 5G. For example, if the use case does not require a data rate of 100 megabits per second or latency of less than 10 milliseconds, it could be met with a 4G solution.

A.2 Key Aspects of 5G

As with previous generations, 5G standards are defined in a set of releases. Key technologies and concepts for 5G are summarized below:

- 3GPP is developing the standards for 5G and has defined a set of releases for 5G. Each release contains new functionality. 3GPP 5G Release 15 (R-15) supports two architecture modes: NSA and SA. NSA systems rely on existing 4G core infrastructure, while SA systems will operate independently on a 5G Next-Gen Core network.
- Cellular network operators have begun with NSA deployments and are not expected to start transitioning to SA deployments until the end of 2020. 5G Phase 2, completed in 3GPP Release-16 (R-16), focuses on enhancing 5G capabilities and addresses wireless/wireline
- convergence, mission-critical services, V2X, 5G satellite access, Local Area Network support in 5G, network slicing, URLLC, IoT, unlicensed spectrum, time-sensitive networking, terminal positioning and location, efficiency, security, streaming services, and network automation.
- To support the different 5G usage scenarios, 5G introduces NR as the new air interface and a cloud-native, service-based architecture for the core network. Changes to the architecture were needed to enable serving a large number of devices (massive IoT) generating intermittent traffic, while also serving a high level of video traffic. Lower latency requirements require architecture changes to facilitate using only the network functions and resources needed for each 5G service.
- Multi-access edge computing will be used to reduce network congestion and application latency. It moves computing and storage functions to the network edge, closer to end users and data.
- 5G will use low-, mid-, and high-band spectrum. Implementation falls into two main categories: below 6 GHz, called "Sub-6," and mmWave above 24 GHz. Sub-6 GHz will be used primarily for large cells and mobility applications, while mmWave will be deployed as small cells and used for high-data rate, ultra-low latency applications. The amount of spectrum bandwidth that can be aggregated is a function of the spectrum bands. For mmWave bands, 5G permits aggregation of up to 800 MHz of spectrum[14]—a capacity improvement of nearly 10 times over existing systems.
- Implementation of 5G will leverage multiple-input, multiple-output (MIMO) antenna technologies and beamforming techniques to improve data speeds and extend coverage range.
- 5G will use network slicing, a technique that enables a physical network's resources to be dynamically partitioned into multiple virtual networks to support different usage scenarios with diverse network requirements.

14 TS 38.101-1 and 38.101-2, section 5.5A for details on carrier aggregation arrangements

Appendix B Federal 5G Initiatives

Agency	SubOrg	Type	Initiative	Subject Area	Notes
DoD	Army	Initiative	Army Computer Hardware Enterprise Software and Solutions (CHESS)	Acquisition	Army's designated Primary Source for commercial IT; including mobile devices, mobile hardware/infrastructure and IoT
DoD	Navy	Program	Department of Navy Wireless Spiral 3	Acquisition	Contract vehicle for acquisition of wireless services, mobile devices, mobile hardware/infrastructure, and IoT
GSA		Initiative	Mobility contracts/FSSI	Acquisition	
GSA		Initiative	Technology Modernization Fund (TMF)	Acquisition	Modernizing Government Technology Act 2017
GSA		Initiative	Master contract for wireless on federal property Executive Order	Acquisition	
HHS	NIH	Initiative	NIH IT Acquisition and Assessment Center (NITAAC) CIO – Commodities and Solutions	Acquisition	Government Wide Acquisition Contract (GWAC) for acquisition of wireless services, mobile devices, mobile hardware/infrastructure, and IoT
HHS	NIH	Initiative	NITAAC CIO - Solutions and Partners	Acquisition	GWAC for acquisition of IoT
NASA		Initiative	NASA SEWP	Acquisition	GWAC authorized by OMB and managed by NASA. vehicle for acquisition of wireless services, mobile devices, hardware/infrastructure, and IoT
Agriculture		Initiative	Evaluation of IoT Precision Agriculture and Drone/GIS Next- gen Application	Infrastructure	Contract vehicle for acquisition of wireless services, mobile devices, mobile hardware/infrastructure, and IoT
Commerce	FirstNet	Initiative	Nationwide Band 14 Public Safety Network Deployment	Infrastructure	
DoD	U.S. Air Force	Pilot	Smart Bases: Maxwell AFB, Nellis AFB, Tyndall AFB + up to 25 total	Infrastructure	Buildouts by AT&T, Verizon include 5G infrastructure, mobility, cloud access, unified communications, voice, broadband, Wi-Fi expansion and an array of connected devices PLUS managed network operations such as compute, storage and edge capabilities.

Agency	SubOrg	Type	Initiative	Subject Area	Notes
DoT		Initiative	Cellular Vehicle to Everything (C-V2X), Automated Driving Systems (ADS), and Intelligent Transportation System Initiatives	Infrastructure	
Energy	Idaho National Laboratory (INL)	Infrastructure	Secure Millimeter Wave Communication Network for Operating Drones	Infrastructure	Researchers at INL have developed a novel 5G wireless network using newly available millimeter wave frequency to operate UAVs with machine-to- machine (M2M) communications and provide an alternative to existing methods with improved RF coverage and resiliency against cyberattacks.
Commerce	NIST	Initiative	Mobile security standards; LTE Security	Policy and Standards	
Commerce	NTIA ITS	Program	Implementation of the IEEE 802.15.22.3 draft standard for Spectrum Characterization and Occupancy Sensing.	Policy and Standards	Current efforts to aggregate spectrum monitoring data are uncoordinated; the purpose of the standards project is to develop a public standard for the control of a distributed network of RF sensors.
DoD	DoD Chief Information Officer (CIO)	Program	DoD 5G Standards Cross-Department Team (CDT)	Policy and Standards	Tech teams established to tackle various 5G standards topics within standards development orgs (3GPP, ATIS, IEEE)
DoD	DoD CIO	Working Group	Five Eyes (FVEY) Defense CIO Forum (DCIOF) Mobility Working Group	Policy and Standards	International partners coordinating standards engagements
DoI		Initiative	Rural Broadband Deployment Executive Order	Policy and Standards	
FCC		Initiative	Protecting Against National Security Threats Through FCC Programs	Policy and Standards	Data call to determine the extent to which equipment and services, including software, produced or provided by Huawei or ZTE, along with their subsidiaries, parents, and/or affiliates, exist in the nation's communications networks

Agency	SubOrg	Type	Initiative	Subject Area	Notes
FCC		Initiative	FAST – Facilitate American Superiority in 5G Technology	Policy and Standards	
FCC		Working Group	FCC Technological Advisory Council, 5G IoT Working Group	Policy and Standards	
WH	National Security Council	Working Group	5G Sub-PCC on ICT Standards	Policy and Standards	Defining strategy for 5G/ICT standards. Coordinating 3GPP engagements across federal agencies.
DHS		Initiative	S&T Unmanned Aerial System (UAS) threat mitigation	R&D	
DHS	S&T	Program	Secure and Resilient Mobile Network Infrastructure R&D	R&D	Broad Agency Announcement for technologies and approaches to address weaknesses in legacy networks, build security in to 5G networks, and provide federal enterprises with visibility into mobile network traffic accessing enterprise systems.
DoD	Under Secretary of Defense for Research and Engineering (USD R&E)	Pilot	DoD '5G to Next G' Pilots Awards for "Tranche 1" DSS, AR/VR, Smart Warehouse, and Nellis Air Force Base	R&D	Tranche 1 awards through National Spectrum Consortium
DoD	USD R&E and U.S. Air Force Warfare Center	Pilot	Nellis Air Force Base Private 5G Network for 5G Testing	R&D	Extending a private network using 5G Communications on Light Trucks. IWRP seeking commercial software prototypes for testing on the private network.
DoD	Army	Program	Fort Carson Transportation Testbed	R&D	Tests the viability of autonomous vehicles and sensor-based technologies in an effort to: reduce military transportation costs, deliver faster services on site, and improve overall public safety

Agency	SubOrg	Type	Initiative	Subject Area	Notes
DoD	DARPA	Program	Open, Programmable, Secure 5G (OPS-5G) program	R&D	Create open-source software and systems enabling secure 5G and subsequent mobile networks
DoD	DARPA	Program	Spectrum Collaboration Challenge (SC2) Joint DoD/NSF Spectrum Sharing Project	R&D	DoD joint venture with NSF PAWR to test allocation of spectrum resources on CBRS spectrum, which will use the DARPA SC2 emulator transferred to NSF.
DoD	DARPA	Program	Millimeter Wave Digital Arrays (MIDAS)	R&D	Seeks to develop element-level digital beamforming that will support emerging multi-beam communications and directional sensing of the electromagnetic environment in the 18-50 GHz band
DoD	DoD CIO	Program	Spectrum Access Research and Development Program (SAR&DP)	R&D	Reduce the risk associated with sharing spectrum purchased by industry and the development of more agile and opportunistic spectrum operations to enable spectrum access in contested and congested environments. Development of new and innovative methods for sharing spectrum and reducing DoD's overall spectrum footprint.
NSF		Initiative	Spectrum Innovation Initiative	R&D	Brings together academic and industrial researchers as well as stakeholders from federal agencies to exchange information and to guide and accelerate the development and maturation of mmWave wireless technology and standards.
NSF		Program	Platforms for Advanced Wireless Research (PAWR)	R&D	Deploy and manage up to four city-scale research testbeds. This $100M public-private partnership is enabling experimental exploration of new wireless devices, communication techniques, networks, systems, and services that will revolutionize the nation's wireless ecosystem.
NSF		Program	NSF/Intel Partnership on Machine Learning for Wireless Networking Systems (MLWiNS)	R&D	Machine Learning (ML) for wireless networking, spectrum management, and distributed ML over wireless edge networks

Agency	SubOrg	Type	Initiative	Subject Area	Notes
NSF		Program	Communications and Information Foundations (CIF) Core Program	R&D	Addresses research and education projects in wireless communications, information theory, signal processing and networking.
NSF		Program	Computer and Network Systems (CNS) Core Program	R&D	Deals with all aspects of computer and network systems with emphasis on 5G and beyond research, cloud computing, and software-defined networking.
NSF		Program	Communications, Circuits and Sensing-Systems (CCSS) Program	R&D	Supports innovative research in circuit and system hardware and signal processing techniques.
NSF		Program	Secure and Trustworthy Cyberspace (SaTC)	R&D	The goals of the SaTC program are aligned with the National Science and Technology Council's Federal Cybersecurity R&D Strategic Plan and National Privacy Research Strategy to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy.
NSF		Program	Spectrum Efficiency, Energy Efficiency and Security and Spectrum and Wireless Innovation enabled by Future Technologies (SWIFT)	R&D	Stimulates innovations in (i) transmitter technologies, such as filters, antennas, switches and amplifiers that must ensure high in-band performance along with ultra-low spurious out-of-band emission, (ii) receiver technologies that must show significant advancement to ensure that receivers can function in the presence of strong interference, (iii) physical layer and medium access control protocols that are not constrained by existing standards (e.g., cellular and Wi-Fi), (iv) SDR technologies that can operate in the passive/active bands beyond current 6 GHz thresholds, and (v) spectrum coexistence methods that go beyond current standard sensing and database management methods.
NSF		Working Group	Millimeter-Wave Research Coordination Network (RCN)	R&D	Convened researchers in academia, industry and government through a series of six workshops

Agency	SubOrg	Type	Initiative	Subject Area	Notes
VA		Initiative	Telemedicine, Connected Health, Smart Medical Devices, AI- assisted Electronic Health Records Palo Alto Health Care System – 5G enabled hospital	R&D	
WH	Office of Science and Technology Policy/ NITRD	Working Group	Wireless Research & Development (WSRD) IWG	R&D	Inventory of wireless spectrum R&D projects.
WH	OSTP/NITRD	Working Group Team	Advanced Wireless Test Platform Team (AWTP)	R&D	Wireless Spectrum R&D IWG Team; aims to provide forum for interagency coordination on wireless test platforms.
DHS	CISA	Initiative	5G Security and Resilience	Security	As the nation's risk advisor, CISA, through the National Risk Management Center (NRMC), is leading risk mitigation efforts by working with government and industry partners to ensure the security and resilience of 5G technology and infrastructure.
Security	As the nation's risk advisor, CISA, through the National Risk	Project	5G Cybersecurity: Preparing a Secure Evolution to 5G	Security	Project will identify several 5G use case scenarios and demonstrate how commercial and open source products can leverage cybersecurity standards and recommended practices for each 5G use case scenario, and how 5G security features can be utilized.
Commerce	NIST	Working Group	5G Security Standards Initiative	Security	Track and Contribute to 5G security standards.
DoD	DoD CIO	Working Group	5G Secure Profile Working Group	Security	Sponsored by DoD and facilitated by MITRE

Agency	SubOrg	Type	Initiative	Subject Area	Notes
Commerce	National	Initiative	Spectrum Management Programs (AWS-1 & AWS-3 Transition, 500 MHz Initiative), Spectrum Sharing, Spectrum Working Groups (mmWave), IoT Strategy	Spectrum	
Commerce	NIST	Working Group	NIST 5G mmWave Channel Model Alliance	Spectrum	
Commerce	NTIA	Working Group	Spectrum Strategy Task Force	Spectrum	Tasked to implement the October 25, 2018 Presidential memorandum, "Developing a Sustainable Spectrum Strategy for America's Future."
Commerce	NTIA	Working Group	NTIA Commerce Spectrum Management Advisory Committee (CSMAC)	Spectrum	
Commerce	NTIA	Working Group	NTIA Spectrum Efficiency Subcommittee	Spectrum	
Commerce	NTIA	Working Group	NTIA/DoD 3450-3550 Spectrum Pipeline Plan (SPP) Study Group	Spectrum	
FCC		Initiative	Spectrum Auctions: mmWave Auction CBRS Auction Future 5G Auctions	Spectrum	Over 14,000 spectrum licenses were awarded in the upper 37, 39, and 47 GHz Bands. The 600 MHz band has been cleared for 5G services. The 5G mid-band spectrum auction for county-based Priority Access Licenses in the 3550-3650 MHz band raised over $4.5 billion. FCC will hold an auction of 3.7-3.98 GHz (C-Band) spectrum in December 2020.
FCC		Working Group	FCC Spectrum Efficiency Work Group (SEWG)	Spectrum	

Agency	SubOrg	Type	Initiative	Subject Area	Notes
DHS	CISA	Working Group	DHS ICT SCRM Task Force	Supply Chain	Four sub-working groups: Information Sharing Threat Evaluation Qualified Bidder lists & Qualified Manufacturer Lists Policy Recommendations to Incentivize Purchase of ICT from Original OEM or Authorized Resellers
DoD	DoD CIO	Working Group	ATIS 5G Supply Chain Working Group	Supply Chain	
DoS		Initiative	5G Clean Networks	Supply Chain	
FCC		Working Group	Communications Security, Reliability and Interoperability Council (CSRIC) VII, Working Group 2: Managing Security Risk in the Transition to 5G	Supply Chain	
FCC	CSRIC (advisory council)	Working Group	CSRIC VII Working Group 3: Managing Security Risk in Emerging 5G Implementations	Supply Chain	

Appendix C Mapping of 5G Technical Specifications to 5G Architecture

5G Component/Feature	Technical Specifications
5G Spectrum bands	▪ 38.101-1 (FR1) ▪ 38.101-2 (FR2)
5G PHY layer	▪ 38.201, 38.202, 38.211, 38.212, 38.213 ▪ 38.214, 38.215
5G Conformance Testing	▪ 38.101, 38.104, 38.141, 38.508, 38.509, 38.521, 38.522, 38.523, 38.533
5G vRAN	▪ 38.401 (DU, CU, logical-RAN node).
5G Call Processing	▪ Procedures for the 5G System, Stage 2, 23.502, (call flows including attach and PDU session establishment, network function, slice, and slice instance) ▪ Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3, 24.501 ▪ 38.304, 38.305, 38.306, 38.307, 37.340.
5G Higher Layers	▪ 38.321, 38.322, 38.323, 38.331, 37.324.
5G Core	▪ 23.501 (Service-based architecture) ▪ 23.503 (Policy and Charging Control) ▪ 24.526 (UE Policy for 5G System)
5G Network Slicing	▪ System Architecture for the 5G System, Stage 2, TS 23.501 (Core Network Slicing Specification) Orchestration and management, TS28.533 ▪ Radio slicing, TS38.300 ▪ Transport Slicing – IETF/3GPP ▫ Binding the S-NSSAI to transport level is done through the Network Slice management framework (VLAN ids) ▪ Enhanced Network Slicing, TR 23.740
5G Security	▪ Security Architecture and Procedures for 5G System, 3GPP TS 33.501 ▪ 3GPP System Architecture Evolution (SAE) Security Architecture, 3GPP TS 33.401 ▪ System Architecture for the 5G System, Stage 2, TS 23.501 (Network Slicing Specification)

List of Acronyms

Acronym	Definition
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5QI	5G QoS Identifier
AERPAW	Aerial Experimentation and Research Platform for Advanced Wireless
AF	Application Function
AFB	Air Force Base
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
AR/VR	Augmented Reality/Virtual Reality
ARPU	Average Revenue Per User
ATIS	Alliance for Telecommunications Industry Solutions
AUSF	Authentication Server Function
AWS	Advanced Wireless Services
AWTP	Advanced Wireless Test Platform
BLER	Block Error Rate
BS	Base Station
CBRS	Citizens Broadband Radio Service
CHESS	Computer Hardware Enterprise Software and Solutions
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CMFA	Continuous Multi-Factor Authentication
CMVP	Cryptographic Module Validation Program
COSMOS	Cloud Enhanced Open Software Defined Mobile Wireless Testbed for City-Scale Deployment
CPRI	Common Public Radio Interface
C-RAN	Cloud RAN
CSMAC	Commerce Spectrum Management Advisory Committee
CSRIC	Communications Security, Reliability and Interoperability Council
CU	Centralized Unit
DARPA	Defense Advanced Projects Research Agency
DCIOF	Defense CIO Forum
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DL	Downlink
DN	Data Network
DNN	Data Network Name
DOC	Department of Commerce
DoD	Department of Defense

Acronym	Definition
DOI	Department of Interior
DoT	Department of Transportation
DSS	Dynamic Spectrum Sharing
DU	Distributed Unit
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
eNB	4G Evolved Node B
EPC	Evolved Packet Core
E-UTRA	Evolved Universal Terrestrial Radio Access
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FirstNet	First Responder Network Authority
FMG	Federal Mobility Group
FOUO	For Official Use Only
FR	Frequency Range
FVEY	Five Eyes
FWA	Fixed Wireless Access
GHz	Gigahertz
gNB	Next-Generation Node B
GSA	General Services Administration
GUTI	Globally Unique Temporary Identifier
GWAC	Government-Wide Acquisition Vehicle
HHS	Health and Human Services
HPA	High Power Amplifier
ICS	Implementation Conformance Statement
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IMSI	International Mobile Subscriber Identity
INL	Idaho National Laboratory
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IQ	In-phase and Quadrature
IT	Information Technology
ITS	Institute for Telecommunication Sciences
ITU-R	International Telecommunications Union-Radiocommunications Sector
IWG	Interagency Working Group
IWRP	Information Warfare Research Project
km	Kilometer
LoS	Line of Sight
LPD	Low Probability of Detection
LPG	Low Probability of Geolocation

Acronym	Definition
LPI	Low Probability of Intercept
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Medium Access Control
MEC	Multi-access Edge Computing
MHz	Megahertz
MIDAS	Millimeter-Wave Digital Arrays
MIMO	Multiple Input, Multiple Output
MitM	Man-in-the-Middle
ML	Machine Learning
MLWiNS	Machine Learning for Wireless Networking Systems
mMTC	Massive Machine-Type Communications
mmWave	Millimeter Wave
MNI	Mobile Network Infrastructure
NAS	Non-Access Stratum
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NEF	Network Exposure Function
NFV	Network Function Virtualization
NIAP	National Information Assurance Partnership
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NITAAC	NIH Information Technology Acquisition and Assessment Center
NITRD	Networking and Information Technology Research and Development
NIWC	Naval Information Warfare Center
NR	New Radio
NR-ARFCN	New Radio Absolute Radio-Frequency Channel Number
NRF	Network Repository Function
NSA	Non-standalone
NSF	National Science Foundation
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NTIA	National Telecommunications and Information Administration
O-DU	O-RAN Distributed Unit
OPS-5G	Open, Programmable, Secure 5G
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
PAWR	Platforms for Advanced Wireless Research
PCC	Policy Coordination Committee
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit

Acronym	Definition
PLMN	Public Land Mobile Network
PMO	Program Management Office
POWDER	Platform for Open Wireless Data-driven Experimental Research
QFI	QoS Flow ID
QoS	Quality of Service
R&D	Research and Development
R-15	Release 15
R-16	Release 16
RACH	Random Access Channel
RAN	Radio Access Network
RCN	Research Coordination Network
RF	Radio Frequency
RIC	Radio Intelligent Controller
RLC	Radio Link Control
RPP	Requests for Prototype Proposals
RRC	Radio Resource Control
RRH	Remote Radio Head
RRM	Radio Resource Management
SA	Standalone
SaTC	Secure and Trustworthy Cyberspace
SBA	Service-Based Architecture
SC2	Spectrum Collaboration Challenge
SCAS	Security Assurance Specification
SCRM	Supply Chain Risk Management
SDAP	Service Data Adaptation Protocol
SDN	Software Defined Networking
SEPP	Security Edge Protection Proxy
SEWG	Spectrum Efficiency Work Group
SEWP	Solutions for Enterprise Wide Procurement
SIEM	Security Information and Event Management
SII	Spectrum Innovation Initiative
SII-Center	National Center for Spectrum Innovation and Workforce Development
SIM	Subscriber Identity Module
SMF	Session Management Function
S-NSSAI	Single NSSAI
SpecEES	Spectrum Efficiency, Energy Efficiency and Security
SPP	Spectrum Pipeline Plan
SSB	Synchronization Signal Block
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SWIFT	Spectrum and Wireless Innovation enabled by Future Technologies
TAC	Technological Advisory Council

Acronym	Definition
TECS	Tactical Edge Communications System
TLS	Transport Layer Security
TMF	Technology Modernization Fund
TR	Technical Report
TS	Technical Specification
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDM	Unified Data Management
UE	User Equipment
UL	Uplink
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communications
USAF	United States Air Force
USD R&E	Under Secretary for Defense Research and Engineering
USF	Universal Service Fund
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VA	Veterans Affairs
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
vRAN	Virtual Radio Access Network
WG	Working Group
WH	White House
WSRD	Wireless Spectrum Research and Development